Centers for Medicare & Medicaid Services

MARS-E Document Suite, Version 2.0

Volume IV: ACA Administering Entity System Security Plan

Version 2.0

November 10, 2015

Foreword

The Centers for Medicare & Medicaid Services (CMS) has assembled a document suite of guidance, requirements, and templates known as the *Minimum Acceptable Risk Standards for Exchanges (MARS-E)*, Version 2.0.

Version 2.0 of the MARS-E document suite consists of four companion documents:

- *Volume I: Harmonized Security and Privacy Framework*, Version 2.0
- *Volume II: Minimum Acceptable Risk Standards for Exchanges*, Version 2.0
- *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*, Version 2.0
- *Volume IV: ACA Administering Entity System Security Plan*, Version 2.0

This Volume IV includes detailed instructions for supplying the contents of a System Security Plan (SSP), which includes:

- Part A, Executive Summary and System Identification
- Part B, the System Security Controls Implementation Plan
- Part C, the System Privacy Controls Implementation Plan
- Part D, SSP Attachments
- Appendix A – IRS Requirements for Safeguarding Federal Tax Information (FTI)
- Appendix B – Security and Privacy Agreements and Compliance Artifacts

Parts B and C include the contents of *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges* for completion of details by Administering Entities.

Any changes to the MARS-E document suite must be approved by the CMS Chief Information Officer and the CMS Chief Information Security Officer (CMS Senior Agency Official for Privacy).

Record of Changes

Version	Date	Author / Owner	Description of Change	CR #
2.0	November 10, 2015	CMS	Version 2.0 for publication	N/A

CR: Change Request

Table of Contents

List of Tables

SSP Instructions

System Security Plan

Security Controls Implementation

Privacy Controls Implementation

Appendix A

Appendix B

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"). These initiatives will benefit millions of Americans by allowing them to readily obtain affordable healthcare services and by enabling employers to offer more cost-effective insurance coverage to their employees.

Protecting and ensuring the confidentiality, integrity, and availability (CIA) of state Marketplace information, common enrollment information, and associated information systems is the responsibility of the states. 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 Exchanges and state IT systems that support the Marketplaces and common enrollment IT systems.

Purpose

This Volume IV of the MARS-E document suite, Version 2.0 provides the System Security Plan for each Administering Entity (AE) responsible for implementing comprehensive security and privacy controls specified in ACA regulations. AEs are required to complete the System Security Plan and document their compliance with mandates of the ACA legislation and Department of Health and Human Services (HHS) Regulations. The System Security Plan is the key tool for describing an AE's IT security and privacy environment for IT systems and for documenting the implementation of security and privacy controls for the protection of all data received, stored, processed, and transmitted by the ACA AE's IT systems and supporting applications. The SSP must be initiated during the initial stages of the life cycle process for IT systems.

The baseline security and privacy requirements for the health insurance exchanges are documented in *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls* of the MARS-E document suite. Volume II of the document suite fully describes the goals and content of the catalog.

The System Security Plan should be reviewed and updated on an "as needed" basis, including annually, and when there are major system modifications that could potentially impact the security and privacy of the AE's information system.

Scope

The System Security Plan consists of two main sections:

- Section 1 contains SSP Instructions for completing the SSP and the two workbooks described in Parts B and C.
- Section 2 contains the requirements for generating the ACA AE System Security Plan content, which has four parts:
  - **Part A – System Identification** provides an overall description of the business process(es) associated with the IT system and an overall description of the IT system environment supporting the business function. It also includes details of the interconnection/information sharing requirements, rules of behavior (ROB), and a

summary of current risks and/or vulnerabilities to the system. The information contained within Part A can also be used for documenting the relevant security controls in Part B and the privacy controls in Part C.

  - **Part B – ACA AE SSP Security Controls Implementation Workbook** documents and describes how the security controls are implemented for each of the controls in the security catalog.
  - **Part C – ACA AE SSP Privacy Controls Implementation Workbook** documents and describes how the privacy controls are implemented for each of the controls in the privacy catalog.
  - **Part D – SSP Attachments** comprise the ACA AE SSP documentation that may be developed and maintained as separate documents but must be included with the SSP for evaluation. The listed attachments are the SSP Equipment List (Attachment A), SSP Software List (Attachment B), Detailed Configuration Setting Standards (Attachment C), SSP Acronyms and Abbreviations (Attachment D), and SSP Glossary (Attachment E).

- **Appendix A – Appendix A, IRS Requirements for Safeguarding Federal Tax Information (FTI)** provides additional IRS security requirements that must be implemented for any agency facilities, information systems, and personnel that receive, process, transmit, or store FTI.
- **Appendix B – MARS-E Security and Privacy Agreements and Compliance Artifacts** provides a list of required security and privacy artifacts and agreements necessary for AE systems to implement throughout the information system life cycle process.

Audience

This document is intended for use by ACA Administering Entities responsible for implementing comprehensive security and privacy controls specified in ACA regulations.

Document Organization

Table Instr-1 presents the organization of the SSP's instructions (Section 1) and content (Section 2).

Table Instr-1. Organization of Volume IV

Section / Part	Description
Section 1: Instructions	
Overall SSP Instructions	The section contains important instructions on planning assumptions and provides definitions of various roles of personnel responsible for the security and privacy of the system.
How to Complete the SSP Workbook	This section provides detailed instructions for completing the control implementation descriptions; it also includes reference samples. These instructions should be used to document the implementation details in Part B and Part C.
Section 2: SSP Content	
Part A – System Identification	
Executive Summary (Optional)	The SSP Author completes this section. The executive summary provides a short, high-level description appropriate for achieving an executive-level understanding of what the system is, what sensitive data it processes, and what key protections have been applied.
System Identification (Template)	The SSP Author completes this section. It contains instructions on the required information for submission, and must be deleted prior to completing and submitting the SSP. Once completed, this section provides an overall description of the business process(es) associated with the IT system and an overall description of the IT system environment supporting the business function.
Part B – Security Controls	
SSP Security Controls Implementation (Workbook)	The section contains the integrated security controls description, including the control number and control requirements description, implementation guidance, related controls requirements, control implementation description, assessment objectives, and assessment procedures. The SSP Author must complete the control implementation procedure following the guidance in Section 1.
Part C – Privacy Controls	
SSP Privacy Controls Implementation (Workbook)	The section contains the integrated privacy controls description, including the control number and control requirements description, implementation guidance, related controls requirements, control implementation description, assessment objectives, and assessment procedures. The SSP Author must complete the control implementation procedure following the guidance in Section 1.
Part D – SSP Attachments	
Additional security and privacy information	Attachments are a way for the Administering Entities to include further information about their systems environment as part of their SSP. This document includes sample attachments for such information, namely SSP Equipment List, SSP Software List, Detailed Configuration Settings, SSP Acronyms and Abbreviations, and SSP Glossary.
Appendix A: IRS Requirements for Safeguarding FTI	This appendix presents the IRS requirements for safeguarding FTI.
Appendix B: MARS-E Security and Privacy Agreements and Compliance Artifacts	This appendix provides a list of security and privacy agreements and compliance artifacts required both before the AE systems enter production stage and when the systems are in the production stage.

Section / Part	Description
Section 1: Instructions	
Overall SSP Instructions	The section contains important instructions on planning assumptions and provides definitions of various roles of personnel responsible for the security and privacy of the system.
How to Complete the SSP Workbook	This section provides detailed instructions for completing the control implementation descriptions; it also includes reference samples. These instructions should be used to document the implementation details in Part B and Part C.
Section 2: SSP Content	
Part A – System Identification	
Master List of Acronyms for MARS-E Document Suite	This master list of acronyms defines the acronyms used in the MARS-E document suite, Version 2.0.
Master Glossary for MARS-E Document Suite	This master glossary defines the key terms used in the MARS-E document suite, Version 2.0.

Section 1: SSP Instructions

Basic Assumptions about SSP for ACA Administering Entity Systems

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

A. **Application.** These requirements apply to all ACA Administering Entities.

B. **Personally Identifiable Information (PII).** All systems will be processing ACA-related PII.

C. **Federal Tax Information (FTI).** Not all systems will be handling FTI. Therefore, instructions for protecting FTI are not covered in the baseline catalog of controls. Appendix A of this document provides a list of IRS safeguarding requirements that must be met in addition to the MARS-E security controls for systems that receive, store, process, or transmit FTI. The SSP must include the documentation of how these controls are implemented.

D. **Outsourcing and Cloud environments.** Most of the systems will be hosted in an outsourced computing facility or cloud environment. In many cases, the Administering Entity will not be the service provider; accordingly, Implementation of Control statements like "The organization …" can involve multiple parties.

E. **Systems Development Life Cycle (SDLC).** All systems will be required to follow an organization-specific SDLC process. Appendix B provides a list of artifacts and agreements required throughout this life-cycle process.

F. **Terminology.** The following includes definitions of terms used throughout the SSP:

- The "organization" is used generally to mean single or multiple parties on the AE side, including the AE or outsourced service provider. Whenever an AE 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 AE 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).
- 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.
- 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 "Business Owner" is the person in the AE organization who is responsible for the mission and ensures the system serves the business needs of the AE.

A completed SSP must provide detailed technical information about the system, must describe the sensitive information that the system processes or maintains, and must 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 state health insurance Exchange, 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 you have addressed all necessary requirements. Once you are confident that all of the necessary information has been annotated in your 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 officers, or equivalents in creating SSPs for the ACA AE Systems. The SSP identifies the following:

- Applicable laws and/or regulations affecting the system;
- The Rules of Behavior 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 of the system;
- Business process(es) associated with the system;
- The system environment;
- System interconnections;
- System security level; and
- Detail control implementation information (the Workbook).

How to Complete the SSP Workbook

The *Volume III: Catalog of Minimum Acceptable Security and Privacy Controls for Exchanges,* Version 2.0 presents the security and privacy controls organized into individual subcategories commonly referred to as "families." The ACA Administering Entity must fully describe how the AE will implement each control requirement as part of the System Security Plan submission.

The following instructions should guide your completion of the comprehensive implementation description of security controls (the Workbook).

- Describe how the security controls are implemented for all of the 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.

Responding to Controls – An Example to Explain the Process

Error! Reference source not found. presents a sample control derived from the Access Control family. It demonstrates the process for properly completing and submitting a compliant System Security Plan.

Each control within the System Security Plan 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. Six primary fields comprise each control and include:

- **Control.** This field establishes the specific requirement(s) that must be met. In **Error! Reference source not found.**, 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 annual review).
- **Guidance.** In simple, conversational language, this field explains the specific intent of the control and then establishes the practical parameters for compliance. In this example, existing, higher-level policies may already fulfil some AC-1 policy and procedural requirements, and therefore, additional effort and expense may be unnecessary.
- **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 controls across the organization. In this case, the AC-1 control related to Policy and Procedure references a Program Management (PM-9) control that addresses Risk Management, indicating a close relationship between these interrelated disciplines.
- **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. In this example, the author should clearly reference specific Access Control 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 annually to ensure that the content is accurate and current.

- **Assessment Objective.** This field explains the requirements of the assessment team and what the reviewing organization will have to evaluate within the system for compliance.
- **Assessment Methods and Objects.** This field further explains the Assessment objective and also identifies specific action steps the Assessment Team must take along with any additional evidence the team may need to collect.

Table Instr-2. Sample Control – AC-1: Access Control Policy and Procedures

AC-1: Access Control Policy and Procedures	
Control	
The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary) within every three hundred sixty-five (365) days: a. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the access control policy and associated access controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for the organization or, conversely, can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information.	
Related Control Requirement(s):	PM-9
Control Implementation Description: «Click here and type text.]»	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy and procedures, other relevant documents or records. **Interview:** Organizational personnel with access control responsibilities; organizational personnel with information security responsibilities.	

Responding to Control Implementation Descriptions

When completing control implementation description fields, the following questions and considerations must be addressed:

- Identify the Control Status (e.g., Implemented, Inherited, Compensated, Planned, Not Applicable)
- Who is responsible for implementing the solution? [Identify the specific point of contact (e.g., the system developer/maintainer) unless a description has been provided to the author.]
- How is the control implemented? Does the implementation satisfy the control requirements?
- How often is the control reviewed and by whom?

Identify the Control Status

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 controls that are planned should be documented in the Plan of Action and Milestones (POA&M).
- **Not Applicable –** 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?

Explain who is responsible for the each control implementation. In some cases, multiple organizations (or parties, persons, or entities) may bear some responsibility. For instance, some security functionality may be outsourced to a subcontractor, while a state employee or organization handles other elements of the same control.

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

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?

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 Tables 3 and 4 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.

Table Instr-3. 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** A security Impact Analysis report is required as part of change reporting to CMS. The Change Reporting Procedures for State-Based Administering Entity Systems established by CMS can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
Guidance
Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security

CM-4: Security Impact Analysis	
Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems.	
Related Control Requirement(s):	CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2

Control Implementation Description: SAMPLE

State IT Department

Control Status: Implemented

The state 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 state customer requires a change that may impact security, a joint meeting is set up between the State 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 State IT Department. The service providers HB Systems and ABC Data Center are responsible for configuration change control for hardware, OS, boundary protection devices.

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 State IT Department Change Management Process.

An audit of this process is performed annually by the State IT Department for all state and contractors supporting the INSUR System.

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the CM-4 control as described in the control requirements and associated implementation standards.

Assessment Methods and Objects

Examine: Configuration management policy; configuration management plan; procedures addressing security and privacy impact analysis for changes to the information system; security and privacy impact analysis documentation; analysis tools and associated outputs; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with responsibilities for determining security and privacy impacts prior to implementation of information system changes; organizational personnel with information security responsibilities; system/network administrators.

Test: Organizational processes for security and privacy impact analysis.

Table Instr-4. 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 AE privacy training and awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures; b. Administer basic privacy training at least annually, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII at least annually; and c. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually.	
Guidance	
Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy compliance. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as PIAs or SORNs for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training. Organizations should consider combining the privacy and security awareness and training programs and control requirements. Organizations should determine how to incorporate privacy awareness and training content into the controls the organization is required to implement under security controls AT-2 - *Security Awareness Training*, AT-3 - Role-Based Security Training, and AT-4 - Security Training Records.	
Related Control Requirement(s):	AR-3, AT-2, AT-3, AT-4, TR-1
Control Implementation Description: SAMPLE **Control Status: Inherited** 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 practives for protecting PII through understanding how security and privacy principles are applied to specific job responsiblities 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;	

AR-5: Privacy Awareness and Training
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.

Section 2: SSP Content

Part A – System Identification (Executive Summary and Template)

Executive Summary (Optional)

A System Security Plan's executive summary should be a short, direct description appropriate for executive-level readership. The summary should provide a high-level understanding of what the system is, what sensitive data it processes and/or stores, and what key protections have been applied. An executive summary is OPTIONAL, but must not exceed one (1) single-spaced page. The general rule is, "the shorter, the better." Please do not restate procedure. Summarize the important, relevant facts about the system's essential business processes, the general security strategy, and the overall security posture as previously described.

"[Click here and type text]"

1. System Identification

1.1 System Name, Title and Location

Provide the system identifier, which includes the official name and/or title of the system, including any commonly used acronyms.

Table SSP-1. System Name, Title, and Location

System Identifier	Response Data
Official System Name:	
System Acronym:	
Provide the street address where the system physically resides.	

1.2 Responsible Organization

Provide contact information for the organization(s) responsible for the system. The following contact information should be provided in Table SSP-2 for internal as well as external organizations.

Table SSP-2. Responsible Organization

Entity	Response Data
Internal	
Name of Organization:	
Address:	
City, State, Zip:	
Contract Number:	
Contract Name:	
External	
Name of Organization:	
Address:	
City, State, Zip:	
Contract Number:	

Entity	Response Data
Contract Name:	

1.3 Designated Contacts

Indicate the names of other key contact personnel who can address inquiries regarding system characteristics and operation. Required contacts include, but are not limited to, Business Owner, System Developer/Maintainer, SSP author, (or equivalent), etc. The SSP should include the following contact information in Table SSP-, Table SSP-, and Table SSP- for each of the Designated Contacts.

Table SSP-3. Designated Contacts: Business Owner

Business Owner	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-Mail:	
Phone Number:	
Contractor contact information (if applicable):	

Table SSP-4. Designated Contacts: System Developer/Maintainer

System Developer/Maintainer	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-Mail:	

System Developer/Maintainer	Response Data
Phone Number:	
Contractor contact information (if applicable):	

Table SSP-5. Designated Contacts: System Security Plan Author

SSP Author	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Contractor contact information (if applicable):	

Identify and add a table for any additional personnel who can address system-related inquiries. Provide titles and contact information for each.

1.4 Assignment of Security and Privacy Responsibility

Identify one (1) primary security Point of Contact (POC) and one (1) alternate or emergency, Point of Contact. The assignment of security responsibility shall include the following information in Table SSP- and Table SSP-. Identify the primary privacy POC and one (1) alternate, or emergency, POC in Table SSP- and Table SSP-, respectively.

Table SSP-6. Primary Security POC

Primary Security POC	Response Data
Name:	
Title:	
Organization:	

Primary Security POC	Response Data
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact: (name, phone & email)	

Table SSP-7. Alternate Security POC

Alternate Security POC	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact (daytime): (name, phone & email)	

Table SSP-8. Primary Privacy POC

Primary Privacy POC	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	

Primary Privacy POC	Response Data
Phone Number:	
Emergency Contact: (name, phone & email)	

Table SSP-9. Alternate Privacy POC

Alternate Security POC	Response Data
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact (daytime): (name, phone & email)	

1.5 System Operational Status

Note in Table SSP-10 whether the system is New, Operational or Undergoing Major Modification.

Table SSP-10. System Operational Status

System Operational Status	Response Data
Select one System Operational Status from the following: New, Operational, or Undergoing a Major Modification.	

1.6 Description of the Business Process

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?).
- **Indicate the organization (internal and external), and the type of data and processing that will be provided by users, if any**.
  - Describe different user roles and associated levels of access to system-related data (read-only, alter, etc.), system-related facilities, and information technology resources.

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

1.7 Description of Operational / System Environment and Special Considerations

1.7.1 Operational Information

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.

"[Click here and type text]"

1.7.2 System Information

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.
- Describe principal software components.
- Describe principal firmware components. (For security and network appliances)

- Describe principal encryption solutions and public key infrastructures.

"[Click here and type text]"

"[Click here to include the system diagram]"

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.

"[Click here and type text]"

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.

"[Click here and type text]"

1.7.3 System Environment

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

Table SSP-11. System Environment

System Environment	Response Data
Is the system owned or leased?	
Is the system operated by the State 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 the state run consolidated data center, provide the name, location and point of contact for the consolidated data center.	
Provide the hours of operation if this is a facility where the system is hosted:	

System Environment	Response Data
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.
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).	
Is FTI being processed or stored in this system?	
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.	

Use Table SSP-11 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, 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?

Use Table SSP-12 to provide more details regarding system users including the following items:

- User types
- Organizations (internal and external) 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 SSP-12. System 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

1.7.4 Architecture and Topology

Describe the architecture of the information system, and include the following information:

- Describe the network connection rules for communicating with external information systems.
- Describe the functional areas within the architecture (presentation, application and data zones, if applicable) and describe how these address information security requirements.

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

1.7.5 System Boundary

Provide a detailed description of the system boundaries and technical components that defend the boundary. The description should contain the following elements:

- Describe the boundary of the information system for security accreditation.
- Describe the hardware, software, and system interfaces (internal and external) to include interconnectivity.
- Describe the network topology.
- Include a logical diagram for system components with system boundaries, if needed, to clarify understanding of the system function and integration.
- Following the logical diagram, describe the information flow or processes within the system that provide access to the data/information.

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

1.7.6 Primary Platforms and Security Software

Describe the primary computing platform(s) used and the principal system components, including hardware, firmware, software, wireless, and communications resources. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.). This will include vendors and versions. Include the following:

- Information concerning a system's hardware and platform(s). Detailed hardware inventories shall be submitted as an attachment.
- Any security-relevant software protecting the system and information.
- In general terms, the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented, rather than listing the controls that are available in the software.

"[Click here and type text]"

1.7.7 Interconnectivity Interfaces, Web Protocols, and Distributed and Collaborative Computing Environments

Describe the Web protocols and distributed, collaborative computing environments (i.e., processes and applications), and include a description of the following:

- The connectivity between modules within the scope of this system.
- For any system that allows individual web-based access (Internet, Intranet, Extranet) to conduct transactions, the following information should be provided:
  - The Uniform Resource Locator for the web-based transaction;
  - E-authentication architecture implemented;
  - E-authentication interoperable product used;
  - Other authentication products used;
  - Number of electronic logons per year;
  - Number of registered users (Government to Government);
  - Number of registered users (Government to Business);
  - Registered users (Government to Citizen);
  - Number of registered internal users; and
- Description of customer groups being authenticated, e.g., Business Partners, Medicare Service Providers, and Beneficiaries).

"[Click here and type text]"

1.7.8 Special Security Concerns – FTI

Indicate if the system receives, stores, processes, or transmits Federal Tax Information. Appendix A provides a list of IRS requirements for safeguarding FTI. These requirements should be documented in the SSP workbook in addition to the MARS-E security and privacy controls for systems that receive, store, process, or transmit FTI information.

"[Click here and type text]"

1.7.9 Other Special Security Concerns

Include any environmental or technical factors that raise special security concerns, such as:

- The physical location of the information system;
- The system is connected to the Internet;
- The system is located in a harsh environment;
- Software is implemented rapidly;
- Software resides on an open network used by the public; and
- Application(s) is/are processed at a facility outside of the state's control.

"[Click here and type text]"

1.8 System Interconnection / Information Sharing

By definition, system interconnection is the direct connection of two or more IT systems for the purposes 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 Federal Data Services Hub (DSH) to exchange data with CMS.

ACA Administering Entity 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 Administering Entity System. Using Table SSP-13, please describe the information sharing agreements in place that govern the data exchange. If not yet finalized, provide the current 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.

Table SSP-13. Interconnections

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

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

1.9 System Security Level

The System Security Level categorization for all ACA Administering Entity Systems has been predetermined to be **Moderat**e.

Describe in general terms the information handled by the system and associated protective measures. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides guidelines for categorizing information and/or information systems.

"[Click here and type text]"

1.10 E-Authentication Assurance Level

Administering Entities are required to ensure that only authorized individuals have access to AE resources. A critical step in this process is establishing confidence in a user's identity through adequate vetting and the provisioning of suitable authentication credentials.

NIST Special Publication (SP) 800-63-2, *Electronic Authentication Guidelines,* defines four (4) levels of assurance for electronic transactions. Table SSP-14 presents the Authentication Requirements by Assurance Levels.

Table SSP-14. Authentication Requirements by Assurance Levels

Authentication Assurance Level	Identity Proofing Requirements (See SP 800-63-2 for full requirements)	Authentication Requirements
Level 1 affords little or no confidence in the asserted identity's validity.	Identity proofing relies on the subscriber's own assertions.	Single factor authentication, such as a username and password, is adequate.
Level 2 provides some confidence in the asserted identity's validity.	Identity proofing requires verifying the individual's government-issued ID or financial account information, and other information.	Single factor authentication, such as a username and password, is adequate.
Level 3 provides high confidence in the asserted identity's validity.	Identity proofing requires verifying the individual's government-issued ID, a financial account information, and other information.	Multi-factor authentication is required.
Level 4 provides very high confidence in the asserted identity's validity.	In-person proofing is required.	Multi-factor authentication is required.

The OMB guidance, which is supplemented by NIST SP 800-63-2, provides agencies with criteria for determining the level of e-authentication assurance required for specific electronic transactions and systems based on the risks and their likelihood of occurrence (e.g., authentication errors and misuse of credentials).

For AE systems, the required level of assurance of a given system is driven by the guidance provided in the *MARS-E Document Suite* and the results of any associated risk assessment.

MARS-E further defines these requirements for e-authentication, and includes level-specific minimum requirements for identity proofing, credential provisioning, authentication tokens, and system protections. Further guidance is also provided in the Electronic Authentication Guidelines for ACA Administering Entity Systems, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .

Indicate the type of E-Authentication Assurance and authentication type used for each user role in the cell for Response Data in Table SSP-15.

Table SSP-15. E-Authentication Assurance Levels

User Role	Assurance Level	Authentication Type
Anonymous Shopper	AL-1	None

1.11 Applicable Laws or Regulations

List any state laws, regulations, specific standards, guidance, or policies governing the creation of ACA-related systems, organizations, and business processes.

"[Click here and type text]"

1.12 Rules of Behavior

Discuss relevant Rules of Behavior (ROB) as they apply to the various user roles as defined in subsection 2.7.3. (The Department of Health and Humans Services Rules of Behavior is a good example.) Describe initial conditions that require users to sign a Rules of Behavior agreement and define how often each user must re-acknowledge the rules. Identify where these conditions and timelines are defined and describe the general rules that apply, which may include, but are not limited to:

- Password complexity / periodicity;
- Changing system data;
- Searching databases;
- Divulging information;
- Tele-work;
- Remote access;
- Connection to the Internet; and
- Assignment and limitation of system privileges.

The ROB must include the consequences of non-compliance and must clearly state the exact behavior expected of each person. Attach Rules of Behavior as an Appendix (if applicable).

"[Click here and type text]"

1.13 Review of Security or Privacy Controls

Provide information regarding any reviews that have been conducted in the past twelve (12) months.

If a security evaluation were conducted within the past twelve (12) months, the following information must be provided:

- The name of the person and organization performing the review;
- The date of the review;
- The purpose of the review;
- A summary of general findings;
- A list of actions taken as a result of the review; and
- A reference to the location of the full report and corrective action plans.

"[Click here and type text]"

Part B – Security Controls Implementation

1.14 Access Control

Table 1. AC-1: Access Control Policy and Procedures

AC-1: Access Control Policy and Procedures	
Control	
The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary) within every three hundred sixty-five (365) days: a. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the access control policy and associated access controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for the organization or, conversely, can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information.	
Related Control Requirement(s):	PM-9
Control Implementation Description: «Click here and type text.]»	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy and procedures, other relevant documents or records. **Interview:** Organizational personnel with access control responsibilities; organizational personnel with information security responsibilities.	

Table 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 IS 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 IS accounts; f. Establishes organizational standards and procedures for creating, enabling, modifying, disabling, and removing IS accounts for each account type. These procedures include the following activities: 1. Authorizing access to the IS based on: (i) A valid access authorization; (ii) Intended system usage; and (iii) Other attributes as required by the organization or associated missions/business functions; 2. Monitoring the use of information system accounts; 3. Notifying account managers: (i) When accounts are no longer required; (ii) When users are terminated or transferred; and (iii) When individual information system usage or need-to-know changes; g. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. **Implementation Standards** 1. Review information system accounts for compliance with account management requirements within every one hundred eighty (180) days, and require annual certification of all accounts within every three hundred sixty-five (365) days. 2. Remove or disable default user accounts. Rename active default accounts. 3. Implement centralized control of user access administrator functions. 4. Regulate the access provided to contractors and define security requirements for contractors.
Guidance
Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with

AC-2: Account Management	
infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example, (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-2 control as described in the control requirements[and associated implementation standards:	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing account management; security plan; information system design documentation, information system configuration settings and associated documentation; list of active information system accounts along with the name of the individual associated with each account; list of guest/anonymous and temporary accounts along with the name of the individual associated with the each account and the date the account expires; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; information system monitoring records with user IDs and last login date; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities. **Test:** Organizational account management processes on the information system; automated mechanisms for implementing account management in accordance with the established implementation standards.	

Table 3. 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.	
Guidance	
The use of automated mechanisms can include, for example, using email or text messaging to automatically notify account managers when users are terminated or transferred, using the information system to monitor account usage, and using telephonic notification to report atypical information system account usage.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective	

AC-2 (1): Automated Information System Account Management
Determine if the organization has implemented all elements of the AC-2 (1) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms implementing account management functions.

Table 4. 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 three hundred sixty-five (365) days.	
Guidance	
This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-2 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of temporary accounts removed and/or disabled; information system-generated list of emergency accounts removed and/or disabled; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms implementing the removal of temporary/emergency accounts.	

Table 5. AC-2 (3): Disable Inactive Accounts

AC-2 (3): Disable Inactive Accounts
Control
a. The information system automatically disables inactive accounts within sixty (60) days; and

AC-2 (3): Disable Inactive Accounts	
b. The organization defines the time period for non-user accounts (e.g., accounts associated with devices such as service accounts).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-2 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of temporary accounts removed and/or disabled; information system-generated list of emergency accounts removed and/or disabled; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms implementing the process for automatically disabling inactive accounts and non-user accounts.	

Table 6. 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).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-2 (4) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; notifications/alerts of account creation, modification, enabling, disabling, and removal actions; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms auditing account creation, modification, enabling, disabling, and removal actions.	

Table 7. AC-2 (7): Role-Based Schemes

AC-2 (7): Role-Based Schemes	
Control	
The organization: a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; b. 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; c. Monitors privileged role assignments as well as application-specific privileged role assignments; and d. Inspects administrator groups, root accounts, and other system-related accounts on demand, and at least once every fourteen (14) days to ensure that unauthorized accounts have not been created. Privileged user roles associated with applications should be inspected every thirty (30) days.	
Guidance	
Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration. Application-privileged user roles are defined based on business functionality and are assigned to users based on their authorized responsibility when interacting with the application. Each role defined within the application identifies various privileges that the user may have based on business function(s).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-2 (7) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and application-specific privileged user and associated roles; information system audit records; audit tracking and monitoring reports; other relevant documents or records. **Interview:** Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms implementing role-based access control requirements for privileged accounts.	

Table 8. 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**

AC-3: Access Enforcement	
1. If encryption is used as an access control mechanism, it must meet FIPS 140-2 compliant encryption standards (see SC-13). 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. 4. When contracting with external service providers, Personally Identifiable Information (PII), as well as software and services that receive, process, store, or transmit PII must be isolated within the service provider environment to the maximum extent possible so that other service provider customers sharing physical or virtual space cannot gain access to such data or applications.	
Guidance	
Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. For minimum authentication requirements, refer to *Electronic Authentication Guidelines for ACA Administering Entity Systems*, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-3 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing access enforcement; information system design documentation; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records. **Interview:** Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms implementing access control policy and procedures; automated mechanisms implementing account management in accordance with established implementation standards.	

Table 9. AC-3 (9): Access Enforcement – Controlled Release

AC-3 (9): Access Enforcement – Controlled Release
Control
The information system does not release information outside of the established system boundary unless: a. The receiving organization information system or system component provides organization security safeguards; and

AC-3 (9): Access Enforcement – Controlled Release
b. The organization defined safeguards consistent with 45 CFR §155.260 Paragraph (b) (2) are used to validate the appropriateness of the information designated for release.
Guidance
Information systems can only protect organizational information within the confines of established system boundaries. Additional security safeguards may be needed to ensure that such information is adequately protected once it is passed beyond the established information system boundaries. Examples of information leaving the system boundary include transmitting information to an external information system or printing the information on one of its printers. In cases where the information system is unable to make a determination of the adequacy of the protections provided by entities outside its boundary, as a mitigating control, organizations determine procedurally whether the external information systems are providing adequate security. Organizations can determine the adequacy of the security provided by external information systems by various means, including, for example, conducting inspections or periodic testing, establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization; however, the means employed should be sufficient to provide consistent adjudication of the security policy to protect the information. This control enhancement requires information systems to employ technical or procedural means to validate the information prior to releasing it to external systems. For example, if the information system passes information to another system controlled by another organization, technical means are employed to validate that the security attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the information system passes information to a printer in an organization-controlled space, procedural means can be employed to ensure that only appropriately authorized individuals gain access to the printer. This control enhancement is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes policy regarding access to the information, and that policy applies beyond the realm of a particular information system or organization. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (b)(2), (b)(2)(v).
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the AC-3 (9) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing access enforcement; information system design documentation; information system configuration settings and associated documentation; list of security safeguards provided by receiving information system or system components; list of security safeguards validating appropriateness of information designed for release; information audit records; other relevant documents or records. **Interview:** Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers; business owners responsible for oversight management of information system(s). **Test:** Automated mechanisms implementing access control policy and procedures for releasing information outside boundaries of the information system.

Table 10. 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.	
Guidance	
Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example, (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); and (ii) employing hardware mechanisms to enforce one-way information flows. 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.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-4 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; information flow control policies; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; and other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers **Test:** Automated mechanisms implementing information flow enforcement policy and procedures.	

Table 11. AC-5: Separation of Duties

AC-5: Separation of Duties	
Control	
The organization: a. Separates duties of individuals as necessary to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Defines information system access authorizations to support separation of duties. **Implementation Standards** 1. Ensure that audit functions are not 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. Ensure that critical mission functions and information system support functions are divided among separate individuals. 4. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups. 5. Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.	
Guidance	
Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example, (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.	
Related Control Requirement(s):	AC-3, AC-6, PE-3, PE-4, PS-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-5 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system access authorizations; information system audit records; and other relevant documents or records. **Interview:** Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with responsibilities for system testing including system developers and security officers. **Test:** Automated mechanisms implementing separation of duties policy and procedures and associated implementation standards.	

Table 12. 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. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information. **Implementation Standards** 1. Disable all file system access not explicitly required for system, application, and administrator functionality. 2. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS 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 CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected.	
Guidance	
Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.	
Related Control Requirement(s):	AC-2, AC 3, AC 5, CM 6, CM 7, PL-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-6 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-related information for which access must be explicitly authorized; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms implementing least privilege functions and supporting implementing standards.	

Table 13. 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 the following list of security functions (deployed in hardware, software, and firmware) 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. **Implementation Standards** 1. The System Owner explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information for authorized personnel, including, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.	
Guidance	
Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.	
Related Control Requirement(s):	AC-17, AC-18, AC-19
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-6 (1) control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. **Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms implementing least privilege functions including the supporting implementation standards.	

Table 14. 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 the following list of security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audit any use of privileged accounts, or roles, for such functions: 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. **Implementation Standards** 1. For service providers, 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, audit any use of privileged accounts, or roles, for such functions.	
Guidance	
This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Examples of service provider security functions include, but are not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, and other privileged functions.	
Related Control Requirement(s):	PL-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-6 (2) control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. **Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms implementing least privilege functions and role-based access controls.	

Table 15. 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).	
Guidance	
Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts, provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.	
Related Control Requirement(s):	CM-6
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-6 (5) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing least privilege; list of system-generated and user defined privileged accounts; list of system administration personnel; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms implementing least privilege functions and monitoring the use of privileged accounts.	

Table 16. 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.	
Guidance	
Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT).	
Related Control Requirement(s):	AU-2
Control Implementation Description: "Click here and type text"	

AC-6 (9): Auditing Use of Privileged Functions
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the AC-6 (9) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing least privilege; information system design documentation; information system configuration settings and associated documentation; list of privileged functions to be audited; list of audited events; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for reviewing least privileges necessary to accomplish specific tasks; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms auditing the execution of privileged functions.

Table 17. 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.	
Guidance	
Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-6 (10) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing least privilege and the execution of privileged functions that include disabling, circumventing, or altering implemented security safeguards/countermeasures; information system design documentation; information system configuration settings and associated documentation; list of privileged functions and associated user account assignments; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms implementing least privilege functions for non-privileged users.	

Table 18. 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. Configure the information system to lock out the user account automatically after three (3) invalid login attempts through either a local or network connection during a fifteen (15)-minute time period. Require the lockout to persist for a minimum of thirty (30) minutes.	
Guidance	
This control applies whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically released after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.	
Related Control Requirement(s):	AC-2, AC 14, IA-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-7 control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing unsuccessful login attempts; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information security responsibilities; system developers; system/network administrators. **Test:** Automated mechanisms implementing access control policy and procedures for unsuccessful logon attempts.	

Table 19. 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:

AC-8: System Use Notification
Warning! This system contains U.S Government information. By using this information system, you are consenting to system monitoring for law enforcement and other purposes. Unauthorized or improper use of, or access to, this computer system may subject you to state and federal criminal prosecution and penalties as well as civil penalties. At any time, the government may intercept, search, and seize any communication or data transiting or stored on this information system. 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.
Guidance
All information systems prominently display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web sites, web pages where substantial personal information from the public is collected, sftp, SSH, or other services accessed. System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the AC-8 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system audit records; user acknowledgements of notification message or banner; information system design documentation; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibility for providing legal advice; system developers. **Test:** Automated mechanisms implementing system use notification.

Table 20. 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. 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.	
Guidance	
Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. A session is defined as an encounter between an end-user interface device (e.g., computer, terminal, process) and an application, including a network logon. One (1) user session is the time between starting the application and quitting. Some systems may require concurrent user sessions to function properly; however, based on the operational needs, automated mechanisms limit the number of concurrent user sessions. It is good practice to have management's approval for any system to have user concurrent sessions. Management should review the need for user concurrent sessions within every three hundred sixty-five (365) days.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-10 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing concurrent session control; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers. **Test**: Automated mechanisms implementing access control policy for the use of concurrent session control.	

Table 21. 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 or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

AC-11: Session Lock	
Guidance	
Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-11 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing session lock; procedures addressing identification and authentication; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms implementing access control policy for session lock.	

Table 22. 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.	
Guidance	
Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-11 (1) control as described in the control requirements.	
Assessment Methods and Objects	

AC-11 (1): Pattern-Hiding Displays
Examine: Access control policy; procedures addressing session lock; display screen with session lock activated; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Information system implementation of Pattern-Hiding Displays.

Table 23. AC-12: Session Termination

AC-12: Session Termination	
Control	
The information system automatically terminates a user session after fifteen (15) minutes of inactivity.	
Guidance	
This control addresses the termination of user-initiated logical sessions in contrast to SC 10, which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.	
Related Control Requirement(s):	SC-10, SC-23
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-12 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; list of conditions or trigger events requiring session disconnect; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms implementing user session termination after fifteen (15) minutes of inactivity.	

Table 24. AC-14: Permitted Actions without Identification or Authentication

AC-14: Permitted Actions Without Identification or Authentication
Control
The organization:

AC-14: Permitted Actions Without Identification or Authentication	
a. Identifies, documents, and provides supporting rationale in the system security plan for user actions not requiring identification or authentication; and b. Configures Information systems to permit public access without first requiring individual identification and authentication only to the extent necessary to accomplish mission objectives.	
Guidance	
This control addresses situations in which organizations determine that no identification or authentication is required in the organizational information systems. Organizations may allow a limited number of user actions without identification or authentication, including, for example, when individuals access public websites or other publicly accessible federal information systems; when individuals use mobile phones to receive calls; or when receiving facsimiles. Organizations also identify actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow bypass of identification or authentication mechanisms. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication, and thus, the values for assignment statements can be none.	
Related Control Requirement(s):	CP-2, IA-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-14 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system user actions that can be performed without identification and authentication; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities.	

Table 25. AC-17: Remote Access

AC-17: Remote Access
Control
a. The organization monitors for unauthorized remote access to the information. Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the organization's CIO or the designated representative. If authorized, the organization: 1. Documents allowed methods of remote access to the information system; 2. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; 3. Authorizes remote access to the information system prior to allowing such connections; and b. Monitors for unauthorized remote access to the information system.
Implementation Standard(s)

AC-17: Remote Access	
1. Require callback capability with re-authentication to verify connections from authorized locations when a secure data communications service network cannot be used. 2. All computers and devices, whether organization-furnished equipment or contractor-furnished equipment, that require any network access to a network or system are securely configured and meet at least the following security requirements: (i) up-to-date system patches, (ii) current anti-virus software, and (iii) functionality that provides the capability for automatic execution of code disabled. 3. Remote connection for privileged functions must be performed using multi-factor authentication following *Electronic Authentication Guidelines for ACA Administering Entity Systems*, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
Guidance	
Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPN) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) VPNs may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. Although organizations may use interconnection security agreements to authorize remote access connections, this control does not require such agreements. Enforcing access restrictions for remote connections is addressed in AC-3.	
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, PE-17, PL-4, SC-10, SI-4
Control Implementation Description: "Click here and type text" »	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-17 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing remote access implementation and usage (including restrictions); configuration management plan; security plan; information system configuration settings and associated documentation; remote access authorizations; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for managing remote access connections; System/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms monitoring and controlling remote access methods.	

Table 26. AC-17 (1): Automated Monitoring/Control

AC-17 (1): Automated Monitoring/Control
Control
The information system monitors and controls remote access methods.

AC-17 (1): Automated Monitoring/Control	
Guidance	
Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).	
Related Control Requirement(s):	AU-2, AU-12
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-17 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; information system monitoring records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms monitoring and controlling remote access methods.	

Table 27. AC-17 (2): Protection of Confidentiality/Integrity Using Encryption

AC-1 7 (2): Protection of Confidentiality/Integrity Using Encryption	
Control	
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	
Guidance	
Use only the CMS-approved encryption standard (see SC-13).	
Related Control Requirement(s):	SC-8, SC-12, SC-13
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-17 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; information system audit records; other relevant documents or records.	

AC-1 7 (2): Protection of Confidentiality/Integrity Using Encryption
Interview: System/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Cryptographic mechanisms protecting confidentiality and integrity of remote access sessions.

Table 28. 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.	
Guidance	
Limiting the number of access control points for remote accesses reduces the attack surface for organizations.	
Related Control Requirement(s):	SC-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-17 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; network architecture diagram; list of all managed network access control points; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms routing all remote access through managed network access control points.	

Table 29. 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"	
Assessment Procedure:	
Assessment Objective	

AC-17 (4): Privileged Commands/Access
Determine if the organization has implemented all elements of the AC-17 (4) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms implementing management of remote access to privileged commands.

Table 30. AC-18: Wireless Access

AC-18: Wireless Access	
Control	
The organization: a. Prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the organization CIO or a designated representative; b. Monitors for unauthorized wireless access to information systems by employing a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system, and c. Establishes for authorized wireless access usage restrictions, configuration/connection requirements, and implementation guidance for wireless access prior to allowing such connections. **Implementation Standard(s)** 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 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; and l. Security Control SI-4 (14), Employ a wireless intrusion “detection/prevention” system (WIDS/WIPS).	
Guidance	
Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.	
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"	
Assessment Procedure:	

AC-18: Wireless Access
Assessment Objective Determine if the organization has implemented all elements of the AC-18 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing wireless access implementation and usage (including restrictions); configuration management plan; security plan; information system design documentation; information system configuration settings and associated documentation; wireless access authorizations; activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records. **Interview:** Organizational personnel responsible for managing wireless access connections or for authorizing, monitoring, or controlling the use of wireless technologies in the information system; organizational personnel with information security responsibilities. **Test:** Wireless access management capability for the information system.

Table 31. 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.	
Related Control Requirement(s):	SC-8, SC-13
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-18 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers. **Test:** Automated mechanisms implementing wireless access authentication and encryption protections to the information system.	

Table 5. AC-19: Access Control for Mobile Devices

AC-19: Access Control for Mobile Devices
Control
The organization:

AC-19: Access Control for Mobile Devices
a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; b. Authorizes, through the CIO, the connection of mobile devices to organizational information systems; c. Employs an approved method of cryptography (see SC-13) to protect Personally Identifiable Information (PII) residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops; d. Monitors for unauthorized connections of mobile devices to information systems; e. Enforces requirements for the connection of mobile devices to information systems; f. Disables information system functionality that provides for automatic execution of code on mobile devices without user direction; g. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and h. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code and virus protection software. **Implementation Standards** 1. The organization defines inspection and preventive measures. 2. Purge/wipe information from mobile devices based on ten (10) consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones, and tablets). Laptop computers are excluded from this requirement. 3. Only organization-owned mobile devices and software can be used to process, access, and store PII.
Guidance
A mobile device is a computing device that (i) has a small form factor to permit easy carrying by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending on the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog, and are allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization controlled.
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"
Assessment Procedure:

AC-19: Access Control for Mobile Devices
Assessment Objective Determine if the organization has implemented all elements of the AC-19 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing access control for portable and mobile device usage (including restrictions); configuration management plan; security plan; information system design documentation; information system configuration settings and associated documentation; authorizations for mobile device connections to organizational information systems; information system audit records; other relevant documents or records. **Interview:** Organizational personnel who monitor for unauthorized mobile device connections to the organization's information systems; organizational personnel using mobile devices to access organizational information systems; system/network administrators; organizational personnel with information security responsibilities. **Test:** Access control capability authorizing mobile device connections to organizational information systems.

Table 33. AC-19 (5): Full-Device / Container-Based Encryption

AC-19 (5): Full-Device / Container-Based Encryption
Control
The organization employs full-device encryption, or container encryption, to protect the confidentiality and integrity of information on approved mobile devices. **Implementation Standards** For mobile devices containing Personally Identifiable Information (PII), employ encryption to protect the confidentiality and integrity of information on mobile devices (e.g., smartphones and laptop computers).
Guidance
A mobile device is a computing device that (i) has a small form factor to permit easy carrying by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending on the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management; device identification and authentication; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog, and are allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization controlled.

AC-19 (5): Full-Device / Container-Based Encryption	
Related Control Requirement(s):	MP-5, SC-13, SC-28

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the AC-19 (5) control as described in the control requirements and associated implementation standard.

Assessment Methods and Objects

Examine: Access control policy; procedures addressing access control for mobile devices; information system design documentation; information system configuration settings and associated documentation; encryption mechanisms and associated configuration documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities for mobile devices; system/network administrators; organizational personnel with information security responsibilities.

Test: Encryption mechanisms protecting confidentiality and integrity of information on mobile devices.

Table 34. AC-20: Use of External Information Systems

AC-20: Use of External Information Systems
Control
For *organizational users* (staff and contractors within the organization), 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, such as Personally identifiable Information (PII), unless explicitly authorized, in writing, by the CIO or designated representative. If authorized, the organization establishes strict terms and conditions for their use. For *non-organizational users* (such as business partners), the Administering Entity organization establishes terms and conditions, consistent with CMS implementation guidance of HHS Regulation 45 CFR 115.260, and in compliance with legal data sharing agreements signed with CMS, for any trust relationships established with other organizations owning, operating, and/or maintaining external information systems. These terms and conditions allow authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems. **Implementation Standards** For Organizational Users: 1. Instruct all personnel working from a non-organization location to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. 2. Limit remote access only to information resources required to complete job duties. 3. Only organization-owned computers and software can be used to process, access, and store Personally Identifiable Information (PII).
Guidance
External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example, (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned

AC-20: Use of External Information Systems	
computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems. For some external information systems (i.e., information systems operated by other organizations), the trust relationships established between those organizations and the originating organization may require no explicit terms and conditions. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between organizations subordinate to those owning organization, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending on the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments. This control does not apply to the use of external information systems to access public interfaces to organizational information systems. Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address at a minimum the types of applications that can be accessed on organizational information systems from external information systems, and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (a)(1)(iii) (A) and (a)(1)(iii) (B).	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-20 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems; system/network administrators; business and/or system owners responsible for oversight management of business partners; administrators responsible for allowing access to organizational information systems; organizational personnel with information security responsibilities. **Test:** Automated mechanisms implementing terms and conditions on use of external information systems.	

Table 35. 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.	
Guidance	
This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls) to avoid compromise of, damage to, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations.	
Related Control Requirement(s):	CA-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-20 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing the use of external information systems; security plan; information system connection or processing agreements; account management documents; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms implementing limits on use of external information systems.	

Table 36. 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. **Implementation Standards** a. Only organization-owned portable storage devices can be used to process, access, and store Personally Identifiable Information. These devices should employ encryption to protect the confidentiality and integrity of information.

AC-20 (2): Portable Storage Devices	
Guidance	
Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how and under what conditions the devices may be used.	
Related Control Requirement(s):	AC-19 (5)
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-20 (2) control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing the use of external information systems; security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for restricting or prohibiting use of organization-controlled storage devices on external information systems; system/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms implementing restrictions on use of portable storage devices.	

Table 37. AC-21: Information Sharing

AC-21: Information Sharing
Control
The organization: a. Facilitates information sharing as defined in 45 CFR §155.260 (e), Privacy and security of personally identifiable information, or "data 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 (as defined in data sharing agreements such as the Computer Matching Agreement or Information Exchange Agreement) 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.
Guidance
This control applies to information that may be restricted in some manner (e.g., privileged medical information or Personally Identifiable Information) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program / compartment. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (a)(1), (a)(2), (a)(4), (b), (e) and (f). There are specific use/disclosure requirements that must be included in agreements that bind Exchanges and non-Exchange entities to comply with privacy and security standards established under §155.260(a)(3), HIPAA, and the IRS Code. Medicaid/CHIP agencies that enter into data sharing agreements must comply with the confidentiality requirements under Section 1942 of the Social Security Act.

AC-21: Information Sharing	
Related Control Requirement(s):	AC-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-21 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); information system design documentation; information system configuration settings and associated documentation; list of users authorized to make information-sharing/collaboration decisions; list of information-sharing circumstances requiring user discretion; other relevant documents or records. **Interview:** Organizational personnel responsible for making information-sharing/collaboration decisions; system/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms or manual processes implementing access authorizations supporting information-sharing/user collaboration decisions.	

Table 38. 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; 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 bi-weekly and removes such information, if discovered.	
Guidance	
In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication.	
Related Control Requirement(s):	AC-3, AC-4, AT-2, AT-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AC-22 control as described in the control requirements.	

AC-22: Publicly Accessible Content
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records; other relevant documents or records. **Interview:** Organizational personnel responsible for managing publicly accessible information posted on organizational information systems; organizational personnel with information security responsibilities. **Test:** Automated mechanisms implementing management of publically accessible content.

1.15 Awareness and Training (AT)

Table 39. AT-1: Security Awareness and Training Policy and Procedures

AT-1: Security Awareness and Training Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A security and privacy awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; b. Procedures to facilitate the implementation of the security and privacy awareness and training policy and associated security and privacy awareness and training controls; c. Security and privacy awareness and training policy; and d. Security and privacy awareness and training procedures. e. Security and privacy awareness and training plan. **Implementation Standards** 1. An initial Security and Privacy awareness and training plan is developed and implemented that addresses all requirements of the security and privacy training program. This plan should cover required policies and procedures and a documented process for implementing basic privacy and awareness training for all organizational users and contractors that includes understanding potential indicators of insider threats. This plan should also include requirements for ensuring personnel with specific roles and responsibilities in information security and privacy undergo more detailed and audience specific security and privacy training.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of security and privacy controls and control enhancements in the AT family. Policy and procedures reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security and privacy policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security and privacy programs in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. CMS provides specific submission requirements and due dates for the training plan in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	PM-9
Control Implementation Description: ** Note: The Security and Privacy Awareness and Training Plan is a required artifact. "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AT-1 control as described in the control requirements.	
Assessment Methods and Objects	

AT-1: Security Awareness and Training Policy and Procedures
Examine: Security and privacy awareness and training policy and procedures; and other relevant documents or records. **Interview:** Organizational personnel with security and privacy awareness and training responsibilities; organizational personnel with information security and privacy responsibilities.

Table 40. 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): a. As part of initial training for new users prior to accessing any system's information; b. When required by system changes, and 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 individuals working on behalf of the organization and involved in managing, using, and/or operating information systems. 2. 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 HHS Regulations and CMS and organization guidance.	
Guidance	
Organizations determine the appropriate content of security and privacy awareness training, and security and privacy awareness techniques, based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and privacy, and to respond to suspected security and privacy incidents. The content also addresses awareness of the need for operations security and privacy related to the organization's information security program. Security and privacy awareness techniques can include, for example, displaying posters, offering supplies inscribed with security and privacy reminders, generating email advisories / notices from senior organizational officials, displaying logon screen messages, and conducting information security and privacy awareness events.	
Related Control Requirement(s):	AT-3, AT-4, PL-4, AR-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AT-2 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects	

AT-2: Security Awareness Training
Examine: Security and privacy awareness and training policy; procedures addressing security and privacy awareness training implementation; appropriate codes of federal regulations; security and privacy awareness training curriculum; security and privacy awareness training materials; security plan; training records; and other relevant documents or records. **Interview:** Organizational personnel with responsibilities for security and privacy awareness training; organizational personnel comprising the general information system user community. **Test:** Automated mechanisms managing security and privacy awareness training.

Table 41. 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 threat.	
Guidance	
Potential indicators and possible precursors of insider threat can include such behaviors as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security and privacy 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, PM-12, PS-3, PS-6
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AT-2 (2) control as described in the control requirements	
Assessment Methods and Objects **Examine:** Security and privacy awareness and training policy; procedures addressing security and privacy awareness training implementation; security and privacy awareness training curriculum; security and privacy awareness training materials; security plan; other relevant documents or records. **Interview:** Organizational personnel that participate in security and privacy awareness training; organizational personnel with responsibilities for basic security and privacy awareness training; organizational personnel with information security and privacy responsibilities.	

Table 42. 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 security and privacy roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; and

AT-3: Role-Based Security Training	
b. When required by information system changes; and within 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.	
Guidance	
Organizations determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals and the specific security and privacy requirements of CMS and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security- and privacy-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of the organization's information security programs. Role-based security and privacy training also applies to contractors providing services to the organization.	
Related Control Requirement(s):	AT-2, AT-4, PL-4, PS-7, SA-3, AR-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AT-3 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Security and privacy awareness and training policy; procedures addressing security and privacy training implementation; codes of federal regulations; security and privacy training curriculum; security and privacy training materials; security plan; training records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for role-based, security- or privacy-related training; and organizational personnel with assigned information system security or privacy roles and responsibilities. **Test:** Automated mechanisms managing role-based security and privacy training.	

Table 43. AT-4: Security Training Records

AT-4: Security Training Records
Control
The organization: a. Documents and monitors individual information system security and privacy training activities including basic security and privacy awareness training and specific information system security and privacy training; and

AT-4: Security Training Records
b. Retains individual training records for a minimum of five (5) years.
Guidance
Procedures and training implementation should: 1. Identify employees with significant information security and privacy responsibilities and provide role-specific training as follows: a. All users of the organization information systems must be exposed to security and privacy awareness materials at least every 365 days. Users of the organization's information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to the information systems and applications. b. Executives must receive training in information security and privacy basics and policy level training in security and privacy planning and management. c. Program and functional managers must receive training in information security and privacy basics; management- and implementation-level training in security and privacy planning and system/application security and privacy management; and management- and implementation-level training in system/ application life-cycle management, risk management, and contingency planning. d. Chief Information Officers (CIO), information security and privacy program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security and privacy officers) must receive training in information security and privacy basics and broad training in security and privacy planning, system and application security and privacy management, system/application life-cycle management, risk management, and contingency planning. e. Information technology (IT) function management and operations personnel must receive training in information security and privacy basics; management- and implementation-level training in security and privacy planning and system/application security and privacy management; and management- and implementation-level training in system/application life-cycle management, risk management, and contingency planning. 2. Provide the organization information systems security and privacy awareness material/exposure to all new employees before allowing them access to the systems. 3. Provide information systems security and privacy refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process. 4. Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.
Related Control Requirement(s): AT-2, AT-3, PM-14
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the AT-4 control as described in the control requirements.
Assessment Methods and Objects **Examine:** Security and privacy awareness and training policy; procedures addressing security and privacy training records; security and privacy awareness and training records; other relevant documents or records. **Interview:** Organizational personnel with security and privacy training record retention responsibilities. **Test:** Automated mechanisms supporting management of security and privacy training records.

1.16 Audit and Accountability (AU)

Table 44. AU-1: Audit and Accountability Policy and Procedures

AU-1: Audit and Accountability Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Audit and Accountability (AU) family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (a)(3)(viii).	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities.	

Table 45. 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 the Implementation Standards; 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

AU-2: Audit Events

c. Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

Implementation Standards

1. Generate audit records for the following auditable events:
   a. Server alerts and error messages;
   b. Log onto system;
   c. Log off system;
   d. Change of password;
   e. All system administrator commands, while logged on as system administrator;
   f. Switching accounts or running privileged actions from another account, (e.g., Linux/UNIX SU or Windows RUNAS);
   g. Creation or modification of super-user groups;
   h. Subset of security administrator commands, while logged on in the security administrator role;
   i. Subset of system administrator commands, while logged on in the user role;
   j. Clearing of the audit log file;
   k. Startup and shutdown of audit functions;
   l. Use of identification and authentication mechanisms (e.g., user ID and password);
   m. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
   n. Remote access outside of the corporate network communication channels(e.g., modems, dedicated Virtual Private Network) and all dial-in access to the system;
   o. Changes made to an applications or database by a batch file;
   p. Application-critical record changes;
   q. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
   r. User log-on and log-off (successful or unsuccessful);
   s. System shutdown and reboot;
   t. System errors;
   u. Application shutdown;
   v. Application restart;
   w. Application errors;
   x. Security policy modifications; and
   y. Printing sensitive information.
2. Subset of Implementation Standard 1, Enable logging for perimeter devices, including firewalls and routers:
   a. User log-on and log-off (successful or unsuccessful);
   b. Log packet-screening denials originating from untrusted networks;
   c. All system administration activities;
   d. Packet-screening denials originating from trusted networks;
   e. Account creation, modification, or deletion of packet filters;
   f. System shutdown and reboot;
   g. System errors; and
   h. Modification of proxy services.
3. Verify that proper logging is enabled to audit administrator activities.
4. 5 U.S.C §552a(c) Accounting of Certain Disclosures:

   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

AU-2: Audit Events	
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.	
Guidance	
An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events that are significant and relevant to the security of information systems and the environments in which those systems operate to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, Personal Identity Verification (PIV) credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. In the definition of auditable events, organizations consider the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-2 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; risk assessment results; information system design documentation; other relevant documents or records. **Interview:** Organizational personnel with auditing and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms implementing information system auditing.	

Table 46. 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** 1. The System Owner reviews and approves the list of auditable events.

AU-2 (3): Reviews and Updates	
Guidance	
Over time, organizations may change their criteria for auditable events. Periodically reviewing and updating the set of audited events is necessary to ensure that the current set remains necessary and sufficient.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-2 (3) control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing auditable events; security plan; list of organization-defined auditable events; auditable events review and update records; information system audit records; information system incident reports; other relevant documents or records. **Interview:** Organizational personnel with auditing and accountability responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting review and update of auditable events.	

Table 47. AU-3: Content of Audit Records

AU-3: Content of Audit Records	
Control	
The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	
Guidance	
Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).	
Related Control Requirement(s):	AU-2, AU-8, AU-12, SI-11, AR-8
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-3 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing content of audit records; information system design documentation; information system configuration settings and associated documentation; list of	

AU-3: Content of Audit Records
organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records. **Interview:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms implementing information system auditing of auditable events.

Table 48. 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.	
Guidance	
Detailed information that organizations may consider in audit records includes for example, full text recording of privileged commands or the individual identities of group account users. Organizations may consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-3 (1) control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing content of audit records; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; security plan; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.	

AU-3 (1): Additional Audit Information
Test: Information system audit capability; automated mechanisms generating specific audit records.

Table 49. 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.	
Guidance	
The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood that such capacity will be exceeded and result in the potential loss or reduction of auditing capability.	
Related Control Requirement(s):	AU-2, AU-5, AU-6, AU-7, AU-11, SI-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-4 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Audit record storage capacity and related configuration settings.	

Table 50. AU-5: Response to Audit Processing Failures

AU-5: Response to Audit Processing Failures
Control
The information system alerts defined personnel or roles (defined in the applicable security plan) in the event of an audit processing failure.
Guidance
Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and reaching or exceeding audit storage capacity. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

AU-5: Response to Audit Processing Failures	
Related Control Requirement(s):	AU-4, SI-12
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-5 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms implementing information system response to audit processing failures.	

Table 51. 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.	
Guidance	
Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.	
Related Control Requirement(s):	
Control Implementation Description: «Click here and type text.]»	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-5 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms implementing audit storage limit warnings.	

Table 52. 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 regularly for indications of inappropriate or unusual activity; 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, and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. 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 on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment. 3. Investigate suspicious activity or suspected violations on the information system, and report findings to appropriate officials and take appropriate action. 4. Use automated utilities to review audit records at least once weekly for unusual, unexpected, or suspicious behavior. 5. Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created. 6. Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days. 7. For service providers, the organization reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials.	
Guidance	
Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of Voice Over Internet Protocol (VoIP). Findings can be reported to organizational entities that include, for example, incident response team, help desk, and information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority.	
Related Control Requirement(s):	AC-2 , AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, 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, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-6 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects	

AU-6: Audit Review, Analysis, and Reporting
Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; risk assessment results; other relevant documents or records. **Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms designed to perform audit review, analysis, and reporting, including the review of network traffic; automated utilities designed to review audit records during specified times outlined in the implementation standards.

Table 53. 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.	
Guidance	
Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits.	
Related Control Requirement(s):	AU-12, PM-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-6 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; procedures for investigating and responding to suspicious activities; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms integrating audit review, analysis, and reporting processes.	

Table 54. 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.

AU-6 (3): Correlate Audit Repositories	
Guidance	
Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness.	
Related Control Requirement(s):	AU-12, IR-4
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective	
Determine if the organization has implemented all elements of the AU-6 (3) control as described in the control requirements.	
Assessment Methods and Objects	
Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system audit records across different repositories; other relevant documents or records. **Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting analysis and correlation of audit records	

Table 55. 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.	
Guidance	
Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.	
Related Control Requirement(s):	AC-5, AU-6
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective	
Determine if the organization has implemented all elements of the AU-7 control as described in the control requirements.	

AU-7: Audit Reduction and Report Generation
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities; organizational personnel with information security responsibilities. **Test:** Audit reduction and report generation capability supporting on-demand audit review, analysis, and reporting.

Table 56. 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.	
Guidance	
Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, Internet Protocol (IP) addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.	
Related Control Requirement(s):	AU-2, AU-12
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-7 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, analysis, and reporting tools; documented audit record criteria establishing events of interest; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with audit reduction and report generation responsibilities; organizational personnel with information security responsibilities; system developers. **Test:** Audit reduction and report generation capability; mechanisms to automatically process audit records for events of interest based on selectable event criteria.	

Table 57. AU-8: Time Stamps

AU-8: Time Stamps
Control
a. The information system: Uses internal system clocks to generate time stamps for audit records; and

AU-8: Time Stamps
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).
Guidance
Time stamps generated by the information system include date and time. Time is commonly expressed in UTC, a modern continuation of GMT, or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.
Related Control Requirement(s): AU-3, AU-12
Control Implementation Description:
"Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the AU-8 control as described in the control requirements.
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms implementing time stamp generation.

Table 58. 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** 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.
Guidance
This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

AU-8 (1): Synchronization with Authoritative Time Source	
Related Control Requirement(s):	AU-12
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-8 (1) control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing time stamp generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms implementing internal information system clock synchronization.	

Table 59. 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.	
Guidance	
Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.	
Related Control Requirement(s):	AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-9 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records. **Interview:** Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms implementing audit information protection.	

Table 60. 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 defines this access in the applicable security plan.	
Guidance	
Individuals with privileged access to an information system who are also the subject of an audit by that system may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.	
Related Control Requirement(s):	AC-5
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-9 (4) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing the protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; system-generated list of privileged users with access to management of audit functionality; access authorizations; access control list; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with auditing and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms managing access to audit functionality.	

Table 61. 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.
Guidance
Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, and approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by (i) authors that they did not author particular documents; (ii) senders that they did not transmit messages; (iii) receivers that they did not receive messages; or (iv) signatories that they did not sign documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

AU-10: Non-Repudiation	
Related Control Requirement(s):	SC-8, SC-12, SC-13, SC-17, SC-23

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the AU-10 control as described in the control requirements.

Assessment Methods and Objects

Examine: Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms implementing non-repudiation capability.

Table 62. 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 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. The organization retains audit records online for at least ninety (90) days and further preserves audit records off-line for a period of ten (10) years.

Guidance

Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.

Related Control Requirement(s):	AU-4, AU-5, AU-9, MP-6, DM-2

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the AU-11 control as described in the control requirements and associated implementation standards.

AU-11: Audit Record Retention
Assessment Methods and Objects **Examine:** Audit and accountability policy; audit record retention policy and procedures; security plan; organization-defined retention period for audit records; audit record archives; audit logs; audit records; other relevant documents or records. **Examine:** Disclosure/access to audit records; audit information; inspection records; other relevant documents or records. **Interview:** Organizational personnel with information system audit record retention responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms supporting audit record retention requirements as outlined in the implementation standards.

Table 63. 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. 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 Standards** 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.	
Guidance	
Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records.	
Related Control Requirement(s):	AC-3, AU-2, AU-3, AU-6, AU-7, AR-8
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-12 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; list of auditable events; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information system audit record-generation responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.	

AU-12: Audit Generation
Test: Automated mechanisms implementing audit record generation capability at all information system components where audit capability is deployed.

Table 64. AU-12 (1): System-Wide/Time-Correlated Audit Trail

AU-12 (1): System-Wide/Time-Correlated Audit Trail	
Control	
The information system compiles audit records from defined information system components (defined in the applicable security plan) into a system-wide (logical or physical), time-correlated audit trail.	
Guidance	
Audit trails are time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.	
Related Control Requirement(s):	AU-8, AU-12
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the AU-12 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; system-wide audit trail (logical or physical); information system audit records; other relevant documents or records. **Interview:** Organizational personnel with audit record generation responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms implementing audit record generation capability.	

Table 65. AU-16: Cross-Organizational Auditing

AU-16: Cross-Organizational Auditing
Control
The organization employs organization-defined methods for coordinating organization-defined audit information among external organizations when audit information is transmitted across organizational boundaries.
Guidance
When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals who requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequently other systems record that the requests emanated from authorized individuals.

AU-16: Cross-Organizational Auditing	
Related Control Requirement(s):	AU-6

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the AU-16 control as described in the control requirements.

Assessment Methods and Objects

Examine: Audit and accountability policy; procedures addressing methods for coordinating audit information among external organizations; information system design documentation; information system configuration settings and associated documentation; methods for coordinating audit information among external organizations; information system audit records; other relevant documents or records.

Interview: Organizational personnel with responsibilities for coordinating audit information among external organizational organizations; organizational personnel with information security responsibilities.

Test: Automated mechanisms implementing cross-organizational auditing (if applicable).

1.17 Security Assessment and Authorization (CA)

Table 66. CA-1: Security Assessment and Authorization Policies and Procedures

CA-1: Security Assessment and Authorization Policies and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within three hundred sixty-five (365) days: a. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; b. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; c. Security assessment and authorization policy; and d. Security assessment and authorization procedures.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. The *Security and Privacy Oversight and Monitoring Guide for Administering Entity (AE) Systems in Operation*, found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/, defines a risk-based approach for ensuring that sensitive information used in support of ACA AE operations is properly protected and safeguarded from improper disclosure, use, or loss. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.280 and 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (a)(5), (b)(2)(iii), and (b)(2)(iv).	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CA-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Security assessment and authorization policies and procedures; and other relevant documents or records. **Interview:** Organizational personnel with security assessment and authorization responsibilities; and organizational personnel with information security responsibilities.	

Table 67. 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 within every three hundred sixty-five (365) days in accordance with the current *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges* , 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 every three hundred sixty-five (365) days, in writing, to the Business Owner 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 Administering Entity's (AE) Authorizing Official issues the authority to operate for all newly implemented, or significantly changed, systems. 2. CMS requires that an independent assessment of all security and privacy controls be conducted every three (3) years or with each major system change 3. The annual security and privacy assessment requirement mandated by CMS requires all security and privacy controls attributable to a system to be assessed over a three (3)-year period. To meet this requirement, a subset of the security and privacy controls shall be tested each year so that all controls are tested during a three (3)-year period. CMS provides guidance for conducting annual security and privacy assessments in the document, *Annual Security and Privacy Attestation Procedures for State-Based ACA Administering Entity Systems* found at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ . 4. The Business Owner notifies CMS within thirty (30) days whenever updates are made to system security and privacy authorization artifacts or when significant role changes occur.
Guidance
Organizations assess security and privacy controls in organizational information system and the environments in which those systems operate as part of (i) initial and ongoing security authorizations; (ii) annual assessments; (iii) continuous monitoring; and (iv) system development life-cycle activities. Security and privacy assessments ensure that (i) information security and privacy are built into organizational information systems; (ii) weaknesses and deficiencies are identified early in the development process; (iii) provision of essential information needed to make risk-based decisions as part of the authorization processes; and (iv) effective compliance with vulnerability mitigation procedures. Assessments are conducted on the implemented security and privacy controls as documented in system security plans and information security and privacy program plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security and privacy posture of information systems during the entire life cycle. Security and privacy assessment reports document assessment results in sufficient detail, as deemed necessary by CMS, to (i) determine the accuracy and completeness of the reports and (ii) whether the security and privacy controls are implemented correctly, operating as intended, and producing the desired outcomes in meeting security and privacy requirements. The requirement for assessing security and privacy controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes (CA-6). Security and privacy assessment results are provided to the individuals or roles appropriate for the types of assessments b conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or the authorizing official's designated representatives.

CA-2: Security Assessments

To satisfy annual assessment requirements, organizations can use assessment results from the following sources, including but not limited to (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life-cycle activities. Organizations ensure that security and privacy assessment results are current, relevant to the determination of security and privacy control effectiveness; and obtained with the appropriate level of assessor independence. Existing security and privacy control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed.

Subsequent to initial authorizations, organizations assess security and privacy controls during continuous monitoring. Organizations establish the security and privacy control selection criteria and subsequently select a subset of the security and privacy controls within the information system and its environment of operation for assessment. An organizational assessment of risk determines those security and privacy controls for more frequent assessment, such as those security and privacy controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical to protecting the organization's operations and assets, individuals, other organizations, and the Nation. All other controls are assessed at least once during the information system's three (3)-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the annual assessment requirement, provided that the results are current, valid, and relevant to determining security and privacy control effectiveness. Vulnerability alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control.

The standard rules of engagement for penetration testing should be coordinated with the privacy office to address unintended disclosure of PII.

This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.280 and 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (a)(5), and (b)(2)(iii).

CMS provides submission requirements and due dates for security assessment requirements in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/.

Related Control Requirement(s):	CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SI-4

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the CA-2 control as described in the control requirements and associated implementation standards.

Assessment Methods and Objects

Examine: Security and privacy assessment and authorization policy; procedures addressing security and privacy assessment planning; procedures addressing security and privacy assessments; security and privacy assessment plan; other relevant documents or records.

Interview: Organizational personnel with security and privacy assessment responsibilities; organizational personnel with information security and privacy responsibilities.

Test: Automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting.

Table 68. CA-2 (1): Independent Assessors

CA-2 (1): Independent Assessors	
Control	
The organization employs assessors or assessment teams with CMS-defined level of independence to conduct security and privacy control assessments of the organization's information system. **Implementation Standard** CMS provides guidance for employing independent assessors in the *Framework of Independent Assessment (IA) of Security and Privacy Controls,* located at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Guidance	
Independent assessors or assessment teams are individuals or groups that conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not (i) create a mutual or conflicting interest with the organizations where the assessments are conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals who are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be usable for such decisions, thereby reducing the need to repeat assessments. CMS provides submission requirements and due dates for the security assessment report (SAR) in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CA-2 (1) control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Security and privacy assessment and authorization policy; procedures addressing security and privacy assessments; security authorization package (including system security plan, security and privacy assessment plan, security and privacy assessment report, plan of action and milestones, authorization statement); other relevant documents or records. **Interview:** Organizational personnel with security and privacy assessment responsibilities; organizational personnel with information security and privacy responsibilities.	

Table 69. 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 ISAs on an ongoing basis to verify enforcement of security requirements; and d. Establishes system-to-system connections with CMS through the Fed2NonFed ISA process. **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 Fed2NonFed ISA process is defined in the Fed2NonFed ISA template found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/.	
Guidance	
This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. The organization authorizing official determines the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same Business Owner, an ISA is not required; instead, interface characteristics between the interconnecting information systems can be described in the security plans for their respective systems. If the interconnecting systems have different Business Owners but the Business Owners are in the same organization, the organizations determine whether a Memorandum of Understanding (MOU) and/or a Service Level Agreement (SLA) are required. Instead of developing an ISA, organizations may choose to incorporate this information into formal contracts, especially if the interconnection is to be established between the organization and a nonfederal (private sector) organization. Risk considerations also include information systems that share the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require ISAs and be subject to additional security controls. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(6). CMS provides ISA submission requirements and due dates in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CA-3 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects	

CA-3: System Interconnections
Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system Interconnection Security Agreements; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements; organizational personnel with information security responsibilities; personnel managing the system(s) to which the Interconnection Security Agreement applies.

Table 70. 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, allow-by-exception” policy for allowing defined information systems that receive, process, store, or transmit Personally Identifiable Information (PII) to connect to external information systems.	
Guidance	
Organizations can constrain information system connectivity to external domains (e.g., websites) by employing deny-all, allow by exception (also known as whitelisting). Organizations determine what exceptions, if any, are acceptable.	
Related Control Requirement(s):	CM-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CA-3 (5) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection agreements; security plan; information system design documentation; information system configuration settings and associated documentation; security assessment report; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibility for managing connections to external information systems; network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms implementing restrictions on external system connections.	

Table 71. CA-5: Plan of Action and Milestones

CA-5: Plan of Action and Milestones
Control
The organization: a. Develops and submits 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

CA-5: Plan of Action and Milestones	
weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; b. Updates and submits 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; and c. Submits an updated POA&M to CMS every three (3) months. **Implementation Standards** 1. The Plan of Action and Milestones template is to be used for reporting POA&Ms to CMS and is found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
Guidance	
Plans of action and milestones are key documents in security authorization packages. CMS provides submission requirements and due dates for the POA&M in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	CA-2, CA-7, CM-4, PM-4
Control Implementation Description: *** Note: The Plan of Action and Milestones is a required artifact. "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CA-5 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records. **Interview:** Organizational personnel with plan of action and milestones development and implementation responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms for developing, implementing, and maintaining plan of action and milestones.	

Table 72. CA-5 (1): Automation Support for Accuracy/Currency

CA-5 (1): Automation Support for Accuracy/Currency	
Control	
The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective	

CA-5 (1): Automation Support for Accuracy/Currency
Determine if the organization has implemented all elements of the CA-5 (1) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; information system audit records; plan of action and milestones; other relevant documents or records. **Interview:** Organizational personnel with plan of action and milestones development and implementation responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms for developing, implementing and maintaining plan of action and milestones.

Table 73. CA-6: Security Authorization

CA-6: Security Authorization
Control
The organization: a. Ensures that the Administering Entity (AE) 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 interconnection security agreement (ISA), the CMS-granted Authority to Connect (ATC) is updated: 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.
Guidance
Security authorizations are official management decisions, conveyed through authorization decision documents, by a representative senior organizational official or executive (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to AE operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Explicit authorization to operate the information system is provided by the organization CIO or his/her designated representative prior to placing a system into operations. Through the security authorization process, the organization CIO is accountable for security risks associated with the operation and use of the information system. Office of Management and Budget (OMB) policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three (3)-year reauthorization requirements, which avoids the necessity for separate reauthorization processes. By employing comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is

CA-6: Security Authorization	
updated on an ongoing basis, providing the organization CIO and information system owners with an up-to-date status of the security state of organizational information systems and operational environments. To reduce the administrative cost of security reauthorization, the CIO uses results of the continuous monitoring processes to the maximum extent possible as the basis for rendering a reauthorization decisions. The specific submission requirements and due dates for the security authorization process including the ISA (Fed2NonFed ISA) can be found in the CMS MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	CA-2, CA-7, PM-9, PM-10
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CA-6 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Security assessment and authorization policy; procedures addressing security authorization; security authorization package [including security plan, security assessment report, plan of action and milestones, and authorization statement(s) from authorizing officials); Interconnection Security Agreement (ISA) and CMS-granted Authority to Connect (ATC) if applicable; other relevant documents or records. **Interview:** Organizational personnel with security authorization responsibilities; personnel with system-to-system connection responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms that facilitate security authorization and updates.	

Table 74. 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, at a minimum; 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 AE 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

CA-7: Continuous Monitoring
CMS has specified continuous monitoring and reporting requirements for AE systems in operation in the *Security and Privacy Oversight and Monitoring Guide for Administering Entity Systems in Operation*, found at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ . Reporting requirements include: 1. Quarterly reporting of Plans of Action & Milestones (POA&M) 2. Annual Security Attestation 3. Reporting of significant changes to the AE system
Guidance
Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms “continuous” and “ongoing” imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/ firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (a)(3)(viii), and (a)(5). CMS provides specific submission requirements and due dates for the continuous monitoring reporting requirements in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .
Related Control Requirement(s): CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SI-2, SI-4
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the CA-7 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Security assessment and authorization policy; procedures addressing security authorization; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; procedures for addressing CMS reporting requirements; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records; security impact analyses; status reports; quarterly reports to CMS of plans of action and milestones; annual security attestations; reports to CMS of significant changes to the AE system; other relevant documents or records. **Interview:** Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security responsibilities; organizational personnel with CMS reporting responsibilities; system/network administrators. **Test:** Mechanisms implementing continuous monitoring and CMS reporting.

Table 75. CA-7 (1): Independent Assessment

CA-7 (1): Independent Assessment	
Control	
The use of independent security assessment agents or teams to monitor security controls is not required; however, if the organization employs assessors or assessment teams with CMS-defined level of independence to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy security control assessment requirements.	
Guidance	
Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring assessments based on continuous monitoring strategies and conducted independently by assessors or assessment teams with appropriate levels of independence. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not (i) create a mutual or conflicting interest with the organizations where the assessments are conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services. CMS guidance for employing independent assessors is provided in the *Framework of Independent Assessment of Security Controls,* located at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ . CMS provides specific submission requirements and due dates required by the independent assessment in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	CA-2
Control Implementation Description: *** Note: The Security Assessment Report (SAR) is a required artifact. "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CA-7 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; and other relevant documents or records. **Interview:** Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security responsibilities.	

Table 76. 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 requirements, and the nature of the information communicated.

CA-9: Internal System Connections	
Guidance	
This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections), including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, such as all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CA-9 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Access control policy; procedures addressing information system connections; system and communications protection policy; security plan; information system design documentation; information system configuration settings and associated documentation; list of components or classes of components authorized as internal system connections; security assessment report; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibility for developing, implementing, or authorizing internal system connections; organizational personnel with information security responsibilities.	

1.18 Configuration Management (CM)

Table 77. CM-1: Configuration Management Policy and Procedures

CM-1: Configuration Management Policy and Procedures
Control
The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. **Implementation Standards** The organization documents the configuration management process and procedures to: 1. Define configuration items at the system and component level (e.g., hardware, software, and workstation); 2. Monitor configurations; and 3. 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).
Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Configuration Management (CM) family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.
Related Control Requirement(s): PM-9
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the CM-1 control as described in the control requirements.
Assessment Methods and Objects **Examine:** Configuration management policy and procedures; configuration management plan; patch management process; relevant documents or records. **Interview:** Organizational personnel with configuration management and control responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Table 78. 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.	
Guidance	
This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters); network topology; and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.	
Related Control Requirement(s):	CM-3, CM-6, CM-8, CM-9, PM-5, PM-7, SA-10
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-2 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; documented baseline configuration for information system components; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; information system configuration settings and associated documentation; change control records; other relevant documents or records. **Interview:** Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for managing baseline configurations; automated mechanisms supporting configuration control of the baseline configuration.	

Table 79. 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; 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

CM-2 (1): Reviews and Updates
d. Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy. **Implementation Standards** The Service Provider reviews and updates the baseline configuration of the information system: 1. Annually; 2. When required due to a significant change; and 3. As an integral part of information system component installations and upgrades.
Guidance
This control requires the organization to review and update baseline configurations defined in CM-1, and update the System Security Plan.
Related Control Requirement(s): CM-5
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the CM-2 (1) control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; procedures addressing information system component installations and upgrades; information system architecture and configuration documentation; information system configuration settings and associated documentation; records of information system baseline configuration reviews and updates; information system component installations/upgrades and associated records; change control records; other relevant documents or records. **Interview:** Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; service providers responsible for maintaining the baseline configuration(s). **Test:** Organizational processes for managing baseline configurations; automated mechanisms supporting review and update of the baseline configuration.

Table 80. 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.
Guidance
Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.
Related Control Requirement(s):
Control Implementation Description:
"Click here and type text"

CM-2 (3): Retention of Previous Configurations
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the CM-2 (3) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; information system configuration settings and associated documentation; copies of previous baseline configuration versions; other relevant documents or records. **Interview:** Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for managing baseline configurations.

Table 81. 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; e. Retains records of configuration-controlled changes to the information system for at least three (3) years; 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 and/or AE 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 system owner coordinates and provides oversight for configuration change control activities through organization-defined configuration change control element (e.g., committee or board) that convenes according to organization-defined frequency and according to organization-defined configuration change conditions. 2. The system owner 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 significant 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 system owner. The means of communication with CMS about significant changes must follow the Change Reporting Procedures for State-Based Administering Entity Systems established by CMS, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ . 4. In establishing contracts with non-Exchange entities, the organization requires the non-Exchange entity to inform the organization of any changes in its administrative, technical, or operational environment defined as material within the contract.

CM-3: Configuration Change Control	
Guidance	
Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, configuration control boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the configuration control boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. "Significant change" is defined in NIST Special Publication 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems.* CMS provides submission requirements and due dates for the Change Report (Change Notification Form) in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-4, SA-10, SI-2, SI-12
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-3 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Configuration management policy; procedures addressing information system configuration change control; configuration management plan; information system architecture and configuration documentation; security plan; change control records; information system audit records; change control audit and review reports; agenda / minutes from configuration change control oversight meetings; notifications of configuration changes to CMS; other relevant documents or records. **Interview:** Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; business and/or system owners; members of change control board or similar. **Test:** Organizational processes for configuration change control; automated mechanisms that implement configuration change control.	

Table 82. 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.
Guidance
Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and

CM-3 (2): Test/Validate/Document Changes	
procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-3 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; information system configuration settings and associated documentation; test records; validation records; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for configuration change control; automated mechanisms supporting and/or implementing testing, validating, and documenting information system changes.	

Table 83. 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. **Implementation Standards** 1. A security Impact Analysis report is required as part of change reporting to CMS. The Change Reporting Procedures for State-Based Administering Entity Systems established by CMS can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
Guidance
Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems.

CM-4: Security Impact Analysis	
CMS provides submission requirements and due dates for the Security Impact Analysis Report in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-4 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing security and privacy impact analysis for changes to the information system; security and privacy impact analysis documentation; analysis tools and associated outputs; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for determining security and privacy impacts prior to implementation of information system changes; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for security and privacy impact analysis.	

Table 84. 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. Processing or storing of Personally Identifiable Information (PII) in test environments is prohibited.	
Guidance	
Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines).	
Related Control Requirement(s):	SA-11, SC-3, SC-7, DM-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-4 (1) control as described in the control requirements.	

CM-4 (1): Separate Test Environments
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing security and privacy impact analysis for changes to the information system; security and privacy impact analysis documentation; information system design documentation; information system architecture and configuration documentation; analysis tools and associated outputs; change control records; information system audit records; evidence of separate information system test and operational environments; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for determining security and privacy impact analysis prior to implementation of information system changes; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Mechanisms supporting the verification of separate test environments for the information system.

Table 85. CM-4 (2): Verification of Security Functions

CM-4 (2): Verification of Security Functions	
Control	
The organization checks the security functions after the information system is changed to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome for meeting the system's security requirements.	
Guidance	
Implementation in this context refers to installing changed code in the operational information system.	
Related Control Requirement(s):	SA-11
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-4 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing security and privacy impact analysis for changes to the information system; security and privacy impact analysis documentation; analysis tools and associated outputs; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for determining security and privacy impacts prior to implementation of information system changes; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for security and privacy impact analysis; automated mechanisms supporting and/or implementing verification of security functions.	

Table 86. 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.	
Guidance	
Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).	
Related Control Requirement(s):	AC-3, AC-5, AC-6, PE-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-5 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; physical access approvals; access credentials; information system design documentation; information system configuration settings and associated documentation; logical access approvals; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for managing access restrictions for change; automated mechanisms implementing enforcement of access restrictions for changes to the information system; automated mechanisms supporting auditing of enforcement actions.	

Table 87. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-5 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; information system configuration settings and associated documentation; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Organizational processes for managing access restrictions for change; automated mechanisms implementing enforcement of access restrictions for changes to the information; automated mechanisms supporting auditing of enforcement actions**.**	

Table 88. 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.	
Guidance	
In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases unknown to developers.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-5 (5) control as described in the control requirements.	
Assessment Methods and Objects	

CM-5 (5): Limit Production/Operational Privileges
Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; security plan; information system design documentation; information system architecture and configuration documentation; information system configuration settings and associated documentation; user privilege reviews; user privilege recertification's; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for managing access restrictions for change; automated mechanisms supporting and/or implementing access restrictions for change.

Table 89. 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; 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. National Institute of Standards and Technology (NIST) b. CMS c. Defense Information Systems Agency (DISA) d. Office of Management and Budget (OMB) 2. If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group, such as The Center for Internet Security (CIS) checklists. 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).
Guidance
Configuration settings are the sets of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, and domain name); workstations; input/output devices (e.g., scanners, copiers, and printers); network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, and sensors); operating systems; middleware; and applications. Security-related parameters are those parameters impacting the security state of information systems, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.

CM-6: Configuration Settings	
Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, and security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB), which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc . The detailed configuration settings are to be submitted as an attachment to the SSP. CMS provides submission requirements and due dates for SSP attachments in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	AC-19, CM-2, CM-3, CM-7, CM-8, SI-4
Control Implementation Description: The detailed configuration settings are to be submitted as an attachment to the SSP. "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-6 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine: C**onfiguration management policy; configuration management plan; procedures addressing configuration settings for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; evidence supporting approved deviations from established configuration settings; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with security configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for managing configuration settings; automated mechanisms that implement, monitor, and/or control information system configuration settings; automated mechanisms that identify and/or document deviations from established configuration settings.	

Table 90. 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.

CM-6 (1): Automated Central Management/ Application/Verification	
Related Control Requirement(s):	CA-7, CM-4

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the CM-6 (1) control as described in the control requirements.

Assessment Methods and Objects

Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; change control records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with security configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers

Test: Organizational processes for managing configuration settings; automated mechanisms implementing the management, application, and verification of configuration settings

Table 91. 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. **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.
Guidance
Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). It is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hypertext Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can use network scanning tools, intrusion detection and

CM-7: Least Functionality	
prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc .	
Related Control Requirement(s):	AC-6, CM-2, RA-5, SA-5, SC-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-7 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; analysis tool outputs; other relevant documents or records. **Interview:** Organizational personnel with security configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes prohibiting or restricting functions, ports, protocols, and/or services; automated mechanisms implementing restrictions or prohibition of functions, ports, protocols, and/or services.	

Table 92. 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; and b. Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.	
Guidance	
The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols.	
Related Control Requirement(s):	AC-18, CM-7, IA-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-7 (1) control as described in the control requirements.	
Assessment Methods and Objects	

CM-7 (1): Periodic Review
Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; documented reviews of functions, ports, protocols, and/or services; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with security configuration management responsibilities; Organizational personnel with responsibilities for reviewing, identifying and eliminating unnecessary functions, ports, protocols, and services on the information system; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for reviewing/disabling nonsecure functions, ports, protocols, and/or services

Table 93. CM-7 (2): Prevent Program Execution

CM-7 (2): Prevent Program Execution	
Control	
The information system prevents program execution in accordance with the list of authorized or unauthorized software programs and rules authorizing the terms and conditions of software program usage.	
Related Control Requirement(s):	CM-8, PM-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-7 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms preventing software program execution on the information system; organizational processes for software program usage and restrictions; automated mechanisms preventing program execution on the information system; automated mechanisms supporting and/or implementing software program usage and restrictions.	

Table 94. 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; and

CM-7 (4): Unauthorized Software/Blacklisting	
c. Reviews and updates the list of unauthorized software programs within every three hundred sixty-five (365) days.	
Guidance	
The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution.	
Related Control Requirement(s):	CM-6, CM-8, PM-5
Control Implementation Description:	
"Click here and type text"	

Table 95. 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: organization-defined information deemed necessary to achieve effective property accountability, which may include hardware inventory specifications (e.g., manufacturer, type, model, serial number, and physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address. 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).
Guidance
Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association and information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, and component owners; and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. The Information System Component Inventory (hardware and software requirements) are required to be submitted as an attachment to the SSP. CMS provides submission requirements and due dates for SSP attachments in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .

CM-8: Information System Component Inventory	
Related Control Requirement(s):	CM-2, CM-6, PM-5, SE-1
Control Implementation Description: The Information System Component Inventory (hardware and software requirements) are required to be submitted as an attachment to the SSP. "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-8 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; inventory reviews and update records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for information system component inventory; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for developing and documenting an inventory of information system components; automated mechanisms supporting and/or implementing the information system component inventory.	

Table 96. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-8 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; inventory reviews and update records; component installation records; component removal records; other relevant documents or records. **Interview:** Organizational personnel with information system installation and inventory responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for updating inventory of information system components; automated mechanisms implementing updating of the information system component inventory.	

Table 97. 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: disables network access by such components/devices and notifies defined personnel or roles (defined in the applicable security plan). **Implementation Standards** In a shared computing facility, the Service Provider: 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.	
Guidance	
This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-8 (3) control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system design documentation; information system configuration settings and associated documentation; information system inventory records; alerts/notifications of unauthorized components within the information system; information system monitoring records; component installation records; change control records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for managing the automated mechanisms implementing unauthorized information system component detection; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Organizational processes for detection of unauthorized information system components; Automated mechanisms for detecting unauthorized components/devices on the information system.	

Table 98. CM-8 (5): No Duplicate Accounting of Components

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

CM-8 (5): No Duplicate Accounting of Components	
The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.	
Guidance	
This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-8 (5) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; component installation records; other relevant documents or records. **Interview:** Organizational personnel with information system inventory responsibilities; organizational personnel with responsibilities for defining information system components within the authorization boundary of the system; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for maintaining the inventory of information system components; automated mechanisms implementing the information system component inventory to ensure no duplication of accounting exists.	

Table 99. CM-9: Configuration Management Plan

CM-9: Configuration Management Plan
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 at organization-defined frequency.

CM-9: Configuration Management Plan	
Guidance	
Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for using configuration management to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes; how to update configuration settings and baselines; how to maintain information system component inventories; how to control development, test, and operational environments; and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system-by-system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. CMS provides submission requirements and due dates for the Configuration Management Plan in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-9 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; configuration management plan; procedures addressing configuration management planning; security plan; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for developing the configuration management plan; organizational personnel with responsibilities for implementing and managing processes defined in the configuration management plan; organizational personnel with responsibilities for protecting the configuration management plan; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for developing and documenting the configuration management plan; organizational processes for identifying and managing configuration items; organizational processes for protecting the configuration management plan; automated mechanisms implementing the configuration management plan; automated mechanisms for managing configuration items; automated mechanisms for protecting the configuration management plan.	

Table 100. CM-10: Software Usage Restrictions

CM-10: Software Usage Restrictions
Control
The organization:

CM-10: Software Usage Restrictions	
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.	
Guidance	
Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	
Related Control Requirement(s):	AC-17, CM-8, SC-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-10 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; procedures addressing software usage restrictions; configuration management plan; security plan; software contract agreements and copyright laws; Software use policy, site license documentation; list of software usage restrictions; software installation policy and procedures, file sharing policy; other relevant documents or records. **Interview:** Organizational personnel with information security responsibilities; system/network administrators; Organizational personnel with software installation responsibilities; organizational personnel with responsibilities for managing software site licenses; organizational personnel responsible for monitoring peer-to-peer file-sharing technology; organizational personnel operating, using, and/or maintaining the information system. **Test:** Organizational process for tracking the use of software protected by quantity licenses; organizational process for controlling/documenting the use of peer-to-peer file sharing technology; automated mechanisms implementing software license tracking; automated mechanisms implementing and controlling the use of peer-to-peer file sharing technology.	

Table 101. 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.
Guidance
Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. There are, however, various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

CM-10 (1): Open Source Software	
Related Control Requirement(s):	AC-17, CM-8, SC-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CM-10 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Configuration management policy; procedures addressing software usage restrictions; configuration management plan; security plan; software contract agreements and copyright laws; Software use policy, site license documentation; list of software usage restrictions; software installation policy and procedures, file sharing policy; other relevant documents or records. **Interview:** Organizational personnel with information security responsibilities; system/network administrators; Organizational personnel with software installation responsibilities; organizational personnel with responsibilities for managing software site licenses; organizational personnel responsible for monitoring peer-to-peer file-sharing technology; organizational personnel operating, using, and/or maintaining the information system. **Test:** Organizational process for tracking the use of software protected by quantity licenses; organizational process for tracking the use of open source software; organizational process for controlling/documenting the use of peer-to-peer file sharing technology; automated mechanisms implementing software license tracking; automated mechanisms implementing and controlling the use of peer-to-peer file sharing technology.	

Table 102. 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 at organization-defined frequency.	
Guidance	
If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Organizations may develop their own policies or adopt those provided by some external entity for governing user-installed software. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.	
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"	
Assessment Procedure:	

CM-11: User-Installed Software
Assessment Objective Determine if the organization has implemented all elements of the CM-11 control as described in the control requirements.
Assessment Methods and Objects **Examine:** Configuration management policy; procedures addressing user installed software; configuration management plan; security plan; information system design documentation; information system configuration settings and associated documentation; list of rules governing user installed software; information system monitoring records; information system audit records; contract agreements, site licenses, file sharing policy; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for governing user-installed software; organizational personnel operating, using, and/or maintaining the information system; organizational personnel monitoring compliance with user-installed software policy; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes governing user-installed software on the information system; automated mechanisms enforcing rules/methods for governing the installation of software by users; automated mechanisms monitoring policy compliance.

1.19 Contingency Planning (CP)

Table 103. CP-1: Contingency Planning Policy and Procedures

CP-1: Contingency Planning Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Contingency Planning (CP) family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (a)(3)(vii), and (a)(4)(iv).	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with contingency planning responsibilities; organizational personnel with information security responsibilities.	

Table 104. 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: 1. Identifies essential organizational missions and business functions and associated contingency requirements;

CP-2: Contingency Plan
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, CMS, 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 and organizational elements identified above; and g. Protects the contingency plan from unauthorized disclosure and modification. **Implementation Standards** 1. The system owner defines a list of key contingency personnel (identified by name and/or by role) and organizational elements for distribution and receipt of the contingency plan and any contingency plan changes. The contingency list includes designated CMS personnel.
Guidance
Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. CMS provides submission requirements and due dates for the Contingency Plan in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .
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, PM-8, PM-11
Control Implementation Description: The Contingency Plan is a required artifact. "Click here and type text"

CP-2: Contingency Plan
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the CP-2 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; evidence of contingency plan reviews and updates; other relevant documents or records. **Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for contingency plan development, review, update, and protection; automated mechanisms for developing, reviewing, updating and/or protecting the contingency plan.

Table 105. 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.	
Guidance	
Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-2 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; business contingency plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; cyber incident response plan; insider threat implementation plans; occupant emergency plans; security plan; other relevant documents or records. **Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security responsibilities; personnel with responsibility for related plans.	

Table 106. 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.	
Guidance	
Capacity planning is needed because different types of threats (e.g., natural disasters or targeted cyber-attacks) can reduce the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-2 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records. **Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security responsibilities.	

Table 107. 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.	
Guidance	
Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may depend on the severity/extent of disruptions to the information system and its supporting infrastructure.	
Related Control Requirement(s):	PE-12
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-2 (3) control as described in the control requirements.	

CP-2 (3): Resume Essential Missions/Business Functions
Assessment Methods and Objects **Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; business impact assessment; other related plans; other relevant documents or records. **Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for resumption of missions and business functions.

Table 108. CP-2 (8): Identify Critical Assets

CP-2 (8): Identify Critical Assets	
Control	
The organization identifies critical information system assets supporting essential missions and business functions.	
Guidance	
Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets to prepare for use of additional safeguards and countermeasures (above and beyond those safeguards and countermeasures routinely implemented) to help ensure the conduct of organizational missions/business functions during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-2 (8) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; business impact assessment; security plan; other relevant documents or records. **Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security responsibilities.	

Table 109. 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: 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.	
Guidance	
Organizations link their contingency training to the assigned roles and responsibilities of organizational personnel to ensure that the training includes the appropriate content and level of detail. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Managers responsible for contingency operations and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented, and the organization should confirm that appropriate training has been completed.	
Related Control Requirement(s):	AT-2, AT-3, CP-2, IR-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-3 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records. **Interview:** Organizational personnel with contingency planning, plan implementation, and training responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for contingency training.	

Table 110. 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 functional exercises 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

CP-4: Contingency Plan Testing	
Implementation Standard. 1. Must produce an after-action report to improve existing processes, procedures, and policies.	
Guidance	
Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. CMS provides submission requirements and due dates for the Contingency Plan Test Results in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-4 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; contingency plan testing and/or exercise documentation; contingency plan test results; after-actin reports associated with contingency plan testing and/or exercise documentation; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for contingency plan testing, reviewing or responding to contingency plan tests; organizational personnel with information security responsibilities. **Test:** Organizational processes for contingency plan testing; automated mechanisms supporting the contingency plan and/or contingency plan testing.	

Table 111. 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.
Guidance
Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements.

CP-4 (1): Coordinate with Related Plans	
Related Control Requirement(s):	IR-8, PM-8

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the CP-4 (1) control as described in the control requirements.

Assessment Methods and Objects

Examine: Contingency planning policy; incident response policy; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan; business continuity plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; cyber incident response plans; occupant emergency plans; security plan; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; organizational personnel with responsibilities for related plans; organizational personnel with information security responsibilities.

Table 112. 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.	
Guidance	
Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.	
Related Control Requirement(s):	CP-2, CP-7, CP-9, CP-10, MP-4

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the CP-6 control as described in the control requirements.

CP-6: Alternate Storage Site
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; primary storage site agreements; other relevant documents or records. **Interview:** Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with information system recovery responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for storing and retrieving information system backup information at the alternate storage site; automated mechanisms supporting and/or implementing storage and retrieval of information system backup information at the alternate storage site.

Table 113. 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.	
Guidance	
Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant.	
Related Control Requirement(s):	RA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-6 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate storage site; primary storage site agreements; other relevant documents or records. **Interview:** Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with information system recovery responsibilities; organizational personnel with information security responsibilities.	

Table 114. 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.

CP-6 (3): Accessibility	
Guidance	
Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane or regional power outage); organizations make these determinations based on organizational assessments of risk. Explicit mitigation actions include, for example, (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites, or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.	
Related Control Requirement(s):	RA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-6 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; list of potential accessibility problems to alternate storage site; mitigation actions for accessibility problems to the alternate storage site; organizational risk assessments; other relevant documents or records. **Interview:** Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with information system recovery responsibilities; organizational personnel with information security responsibilities.	

Table 115. CP-7: Alternate Processing Site

CP-7: Alternate Processing Site
Control
The organization: a. Establishes an alternate processing site as well as the necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site. **Implementation Standards** 1. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within a resumption time period consistent with the recovery time objectives defined by the business owner in the contingency plan.
Guidance
Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in

CP-7: Alternate Processing Site	
contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Equipment and supplies required to resume operations within the organizationally defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with the organization's recovery time objectives.	
Related Control Requirement(s):	CP-2, CP-6, CP-8, CP-9, CP-10, MA-6
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-7 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; security plan; primary processing site agreements; spare equipment and supplies inventory at alternate processing site; equipment and supply contracts; service level agreements; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for contingency planning and/or alternate site arrangements; organizational personnel with information security responsibilities. **Test:** Organizational processes for recovery at the alternate site; automated mechanisms supporting and/or implementing recovery at the alternate processing site.	

Table 116. CP-7 (1): Separation from Primary Site

CP-7 (1): Separation from Primary Site	
Control	
The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.	
Guidance	
Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant.	
Related Control Requirement(s):	RA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-7 (1) control as described in the control requirements.	

CP-7 (1): Separation from Primary Site
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; primary processing site agreements; other relevant documents or records. **Interview:** Organizational personnel with contingency plan alternate processing site responsibilities; organizational personnel with information system recovery responsibilities; organizational personnel with information security responsibilities.

Table 117. CP-7 (2): Accessibility

CP-7 (2): Accessibility	
Control	
The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
Guidance	
Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane or regional power outage); organizations make these determinations based on organizational assessments of risk.	
Related Control Requirement(s):	RA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-7 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; primary processing site agreements; list of potential accessibility problems to the alternate processing site; mitigation actions for accessibility problems to the alternate processing site; other relevant documents or records. **Interview:** Organizational personnel with contingency plan alternate processing site responsibilities; organizational personnel with information system recovery responsibilities; organizational personnel with information security responsibilities.	

Table 118. CP-7 (3): Priority of Service

CP-7 (3): Priority of Service
Control
The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).
Guidance

CP-7 (3): Priority of Service	
Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-7 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; service-level agreements; other relevant documents or records. **Interview:** Organizational personnel with contingency plan alternate processing site responsibilities; organizational personnel with information system recovery responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements.	

Table 119. CP-8: Telecommunications Services

CP-8: Telecommunications Services	
Control	
The organization establishes alternate telecommunications services as well as 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** a. Ensure alternate telecommunications Service Level Agreements (SLA) are in place to permit resumption of system Recovery Time Objectives (RTO) and business function Maximum Tolerable Downtimes (MTD). b. 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.	
Guidance	
This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.	
Related Control Requirement(s):	CP-2, CP-6, CP-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	

CP-8: Telecommunications Services
Assessment Objective Determine if the organization has implemented all elements of the CP-8 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; list of essential missions and business functions; other relevant documents or records. **Interview:** Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with information system recovery responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements; business and/or system owners. **Test:** Automated mechanisms supporting telecommunications requirements for primary and alternate processing and storage sites.

Table 120. 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.	
Guidance	
Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-8 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing primary and alternate telecommunications services; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; other relevant documents or records. **Interview:** Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with information system recovery responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements. **Test:** Automated mechanisms supporting telecommunications.	

Table 121. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-8 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing primary and alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records. **Interview:** Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with information system recovery responsibilities; primary and alternate telecommunications service providers; organizational personnel with information security responsibilities.	

Table 122. 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. Ensure that a current, retrievable, copy of Personally Identifiable Information (PII) is available before movement of servers. 3. (Cloud environments) The system owner shall determine what elements of the cloud environment require the Information System Backup control. 4. (Cloud environments) The system owner determines how Information System Backup will be verified and the appropriate periodicity of the check.
Guidance

CP-9: Information System Backup	
System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. The transfer rate of backup information to an alternate storage site (if so designated) is guided by the organization's recovery time objectives and recovery point objectives. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time.	
Related Control Requirement(s):	CP-2, CP-6, MP-4, MP-5, SC-13
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-9 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; security plan; information system configuration settings and associated documentation; backup storage location(s); information system backup logs or records; other relevant documents or records. **Interview:** Organizational personnel with information system backup responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for conducting information system backups; automated mechanisms supporting and/or implementing information system backups.	

Table 123. CP-9 (1): Testing for Reliability/Integrity

CP-9 (1): Testing for Reliability/Integrity	
Control	
The organization tests backup information following each backup to verify media reliability and information integrity. **Implementation Standards** 1. The organization tests backup information at least annually.	
Related Control Requirement(s):	CP-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-9 (1) control as described in the control requirements and associated implementation standards.	

CP-9 (1): Testing for Reliability/Integrity
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; contingency plan test documentation; contingency plan test results; procedures addressing information system backup; information system backup test results; security plan; backup storage location(s); other relevant documents or records. **Interview:** Organizational personnel with information system backup responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for conducting information system backups; automated mechanisms supporting and/or implementing the testing for reliability/integrity of information system backups.

Table 124. 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 Standards** 1. 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.	
Guidance	
Recovery is executing information system contingency plan activities to restore the organization's missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures.	
Related Control Requirement(s):	CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-10 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; information system backup test results; contingency plan test results; contingency plan test documentation; redundant secondary system for information system backups; location(s) of redundant secondary backup	

CP-10: Information System Recovery and Reconstitution
system(s); procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records. **Interview:** Organizational personnel with contingency planning, recovery, and/or reconstitution responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes implementing information system recovery and reconstitution operations; automated mechanisms supporting and/or implementing information system recovery and reconstitution operations.

Table 125. CP-10 (2): Transaction Recovery

CP-10 (2): Transaction Recovery	
Control	
The information system implements transaction recovery for transaction-based systems.	
Guidance	
Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the CP-10 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; contingency plan test documentation and test results; information system transaction recovery records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibility for transaction recovery; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing transaction recovery capability.	

1.20 Identification and Authentication (IA)

Table 126. IA-1: Identification and Authentication Policy and Procedures

IA-1: Identification and Authentication Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Identification and Authentication (IA) family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information. Reference CMS guidance provided in the *Electronic Authentication Guidelines for ACA Administering Entity Systems*, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Identification and authentication policy and procedures; and other relevant documents or records. **Interview:** Organizational personnel with identification and authentication responsibilities; organizational personnel with information security responsibilities.	

Table 127. IA-2: 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**

IA-2: Identification and Authentication (Organizational Users)	
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. 3. Follow CMS guidance provided in the *Electronic Authentication Guidelines for ACA Administering Entity Systems*, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Guidance	
Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors and guest researchers). This control applies to all accesses other than (i) accesses that are explicitly identified and documented in AC-14, and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPN) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-2 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; and other relevant documents or records; other relevant documents or records. **Interview:** Organizational personnel with information system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with account management responsibilities; system developers. **Test:** Organizational processes for uniquely identifying and authenticating users; automated mechanisms supporting and/or implementing identification and authentication capability.	

Table 128. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-2 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; and other relevant documents or records; information system audit records; list of information system accounts (including privileged accounts); other relevant documents or records. **Interview:** Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing multifactor authentication capability for network access to privileged accounts.	

Table 129. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-2 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of non-privileged information system accounts; other relevant documents or records.	

IA-2 (2): Network Access to Non-Privileged Accounts
Interview: Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing multifactor authentication capability for network access to non-privileged accounts.

Table 130. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-2 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts including privileged accounts; other relevant documents or records. **Interview:** Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing multifactor authentication capability for local access to privileged accounts.	

Table 131. 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.
Guidance
Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

IA-2 (8): Network Access to Privileged Accounts – Replay Resistant	
Related Control Requirement(s):	

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the IA-2 (8) control as described in the control requirements.

Assessment Methods and Objects

Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of privileged and non-privileged information system accounts; other relevant documents or records.

Interview: Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing identification and authentication capability; automated mechanisms supporting and/or implementing replay resistant authentication mechanisms.

Table 132. 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, assuring that one of the factors is provided by a device separate from the system gaining access.

Implementation Standards

Reference CMS guidance provided in the *Electronic Authentication Guidelines for ACA Administering Entity Systems*, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .

Guidance

Requiring a device that is separate from the information system in order to gain remote access to privileged/non-privileged accounts for one of the factors during multifactor authentication reduces the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users.

Related Control Requirement(s):	AC-6

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the IA-2 (11) control as described in the control requirements and associated implementation standards.

Assessment Methods and Objects

IA-2 (11): Remote Access – Separate Device
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of privileged and non-privileged information system accounts; other relevant documents or records. I**nterview:** Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing "multifactor authentication using a separate device".

Table 133. 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 before establishing a connection that, at a minimum, use shared information [i.e., Media Access Control (MAC) or Internet Protocol (IP) address] and access control lists to control remote network access. **Implementation Standards** 1. The organization defines a list a specific devices and/or types of devices approved and accepted for identification and authentication management.	
Guidance	
Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information [e.g., Media Access Control (MAC) or Transmission Control Protocol (TCP)/IP addresses] for device identification or organizational authentication solutions [e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP), Radius server with EAP-Transport Layer Security (TLS) authentication, Kerberos] to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. **Note:** At a minimum, information systems should be filtered by MAC and/or IP address when accessing remote systems.	
Related Control Requirement(s):	AC-17, AC-18, AC-19, CA-3, IA-4, IA-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-3 control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.	

IA-3: Device Identification and Authentication
Interview: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing device identification and authentication capability.

Table 134. 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 at least three (3) years has expired; 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 prevents reuse of user or device identifiers for at least two (2) years and disables the user identifier after ninety (90) days of inactivity. 2. The organization defines time period of inactivity for device identifiers.	
Related Control Requirement(s):	IA-2, IA-3, IA-5, IA-8
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-4 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records. **Interview:** Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers **Test:** Automated mechanisms supporting and/or implementing identifier management.	

Table 135. 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); 2. Personal Identity Verification (PIV)-compliant access cards are valid for no longer than five (5) years; and 3. Public Key Infrastructure (PKI) certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years; 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 changes.	
Guidance	
Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, and files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-5 control as described in the control requirements.	

IA-5: Authenticator Management
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system authenticator types; change control records associated with managing information system authenticators; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for determining initial authenticator content or authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Automated mechanisms supporting and/or implementing authenticator management capability.

Table 136. 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/Privileged Accounts: Eight (8) characters; at least one numeric and at least one special character; a mixture of at least one uppercase and at least one lowercase letter; 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 = 60/60/180 3. MinimumPasswordLength = 8/8/15 e. Enforces at least four (4) changed characters or as determined by the information system (where possible) when new passwords are created; f. Stores and transmits only cryptographically protected passwords; g. Prohibit password reuse for 24 generations; and h. Password-protect system initialization (boot) settings	
Guidance	
This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute=-force attacks against passwords, organizations may also consider salting passwords. Mobile devices are excluded from the password complexity requirement.	
Related Control Requirement(s):	IA-6
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective	

IA-5 (1): Password-Based Authentication
Determine if the organization has implemented all elements of the IA-5 (1) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing password-based authenticator management capability.

Table 137. 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.	
Guidance	
Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses. For Personal Identity Verification cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing.	
Related Control Requirement(s):	IA-6
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-5 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; other relevant documents or records. **Interview:** Organizational personnel with PKI-based, authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing PKI-based, authenticator management capability.	

Table 138. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-5 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; registration process for receiving information system authenticators; list of authenticators requiring in-person registration; list of authenticators requiring trusted third party registration; PKI certification revocation lists; authenticator registration documentation; other relevant documents or records. **Interview:** Organizational personnel with authenticator management responsibilities; registration authority; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing authenticator management capability; automated mechanisms implementing authentication in applications.	

Table 139. 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.	
Guidance	
Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This holds true if that representation is an encrypted version of something else (e.g., a password).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-5 (7) control as described in the control requirements.	

IA-5 (7): No Embedded Unencrypted Static Authenticators
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; other relevant documents or records. **Interview:** Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing authenticator management capability; automated mechanisms implementing authentication in applications.

Table 140. 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.	
Guidance	
Hardware token-based authentication typically refers to the use of Public Key Infrastructure (PKI)-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-5 (11) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing authenticator management; information; security plan; system design documentation; information system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; automated mechanisms employing hardware token-based authentication for the information system; list of token quality requirements; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing hardware token-based authenticator management capability.	

Table 141. 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.	
Guidance	
The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components this threat may be less significant, for example, mobile devices with 2 to 4-inch screens, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.	
Related Control Requirement(s):	PE-18
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IA-6 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information security responsibilities; system/network administrators; system developers. **Test:** Automated mechanisms supporting and/or implementing the obscuring of feedback of authentication information during authentication.	

Table 142. 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.
Guidance
Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

IA-7: Cryptographic Module Authentication	
Related Control Requirement(s):	SC-12, SC-13

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the IA-7 control as described in the control requirements.

Assessment Methods and Objects

Examine: Identification and authentication policy; procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with responsibility for cryptographic module authentication; organizational personnel with information security responsibilities; system/network administrators; system developers.

Test: Automated mechanisms supporting and/or implementing cryptographic module authentication.

Table 143. 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).

Implementation Standards

Follow CMS guidance provided in the *Electronic Authentication Guidelines for ACA Administering Entity Systems*, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .

Guidance

Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users.

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"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the IA-8 control as described in the control requirements and associated implementation standards.

Assessment Methods and Objects

IA-8: Identification and Authentication (Non-Organizational Users)
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records. **Interview:** Organizational personnel with information system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with account management responsibilities. **Test:** Automated mechanisms supporting and/or implementing identification and authentication capability.

1.21 Incident Response (IR)

Table 144. IR-1: Incident Response Policy and Procedures

IR-1: Incident Response Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the incident response policy and associated incident response controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of the Incident Response (IR) family. Policy and procedures reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The IR procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii).	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy and procedures; and other relevant documents or records. **Interview:** Organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities.	

Table 145. 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 ninety (90) days 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.

IR-2: Incident Response Training	
The organization: a. Identifies employees with significant information security responsibilities and provides role-specific training in accordance with NIST standards and guidance; b. Includes user training in the identification and reporting of suspicious activities, both from external and internal sources; c. Exposes all information systems users (i.e., employees, contractors, students, guest researchers, visitors, and others who may need access to information systems and applications) to security awareness materials addressing IR response associated with the roles. For example, regular users may only need to know whom to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. d. Provides information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees uses or processes and their role.	
Guidance	
The organization provides incident response training that is linked to personnel assigned roles and responsibilities to ensure the training includes the appropriate content and level of detail. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii).	
Related Control Requirement(s):	AT-3, CP-3, IR-8, AR-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-2 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing incident response training; incident response training curriculum; incident response training materials; security plan; incident response plan; incident response training records; and other relevant documents or records. **Interview:** Organizational personnel with incident response training and operational responsibilities: organizational personnel with information security responsibilities.	

Table 146. IR-3: Incident Response Testing

IR-3: Incident Response Testing
Control
The organization: a. 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; b. Must produce an after-action report to improve existing processes, procedures, and policies; c. Need not conduct a formal test if the organization actively exercises its response capability using real incidents.

IR-3: Incident Response Testing	
Guidance	
Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii).	
Related Control Requirement(s):	CP-4, IR-8
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-3 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; security plan; other relevant documents or records. **Interview:** Organizational personnel with incident response testing responsibilities; organizational personnel with information security responsibilities.	

Table 147. 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.	
Guidance	
Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii).	
Related Control Requirement(s):	
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-3 (2) control as described in the control requirements.	

IR-3 (2): Coordination with Related Plans
Assessment Methods and Objects **Examine:** Incident response policy; contingency planning policy; procedures addressing incident response testing; incident response testing documentation; incident response plan; business continuity plans; contingency plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; occupant emergency plans; security plan; other relevant documents or records. **Interview:** Organizational personnel with incident reporting responsibilities; organizational personnel with responsibilities for testing organizational plans related to incident response testing; organizational personnel with information security responsibilities.

Table 148. IR-4: Incident Handling

IR-4: Incident Handling	
Control	
The organization: a. Implements an incident handling capability using the current Administering Entity (AE) organization Procedure for Incident Handling; b. Coordinates incident handling activities with contingency planning activities; c. Documents relevant information related to an security incident according to the current AE organization and ACA-required procedures; d. Preserves evidence through technical means, including secured storage of evidence media and "write" protection of evidence media; uses sound forensics processes and utilities that support legal requirements; And determines and follows chain of custody for forensic evidence; e. Identifies vulnerability exploited during a security incident; f. Implements security safeguards to reduce risk and vulnerability exploit exposure; g. Ensures that the individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information processed, stored, and transmitted by the information system; and h. Incorporates lessons learned from ongoing incident handling activities into AE incident response procedures, training, and testing, and implements the resulting changes accordingly. **Implementation Standards** Follow CMS guidance for Incident Handling, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Guidance	
Organizations recognize that incident response capability depends on the capabilities of organizational information systems and the mission/business processes supported by those systems. Therefore, incident response is part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident-handling capability encompasses coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii).	
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"	
Assessment Procedure:	

IR-4: Incident Handling
Assessment Objective Determine if the organization has implemented all elements of the IR-4 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Incident response policy; contingency planning policy; procedures addressing incident handling; incident response plan; incident response plan; contingency plan; security plan; other relevant documents or records. **Interview:** Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities; organizational personnel with information security responsibilities. **Test:** Incident handling capability for the organization.

Table 149. 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.	
Guidance	
Automated mechanisms supporting incident handling processes include, for example, online incident management systems. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-4 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; information system design documentation; information system configuration settings and associated documentation; information system audit records; incident response plan; security plan; other relevant documents or records. **Interview:** Organizational with incident handling personnel responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms that support and/or implement the incident handling process.	

Table 150. IR-5: Incident Monitoring

IR-5: Incident Monitoring
Control
The organization tracks and documents information system security incidents.

IR-5: Incident Monitoring	
Guidance	
Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii).	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-5 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; security plan; other relevant documents or records. **Interview:** Organizational personnel with incident monitoring responsibilities; organizational personnel with information security responsibilities. **Test:** Incident monitoring capability for the organization; automated mechanisms supporting and/or implementing tracking and documenting of system security incidents.	

Table 151. 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 Administering Entity (AE) organization Incident Handling Procedure and ACA incident handling process available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ and b. Reports security incident information to designated authorities.
Guidance
The intent of this control is to address both specific incident reporting requirements within an AE organization and the formal ACA incident reporting requirements. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a) (3) (viii).

IR-6: Incident Reporting	
Related Control Requirement(s):	IR-7
Control Implementation Description: "Click here and type text"	
Assessment Objective Determine if the organization has implemented all elements of the IR-6 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; security plan; other relevant documents or records. **Interview:** Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities; personnel who have/should have reported incidents; personnel (authorities) to whom incident information is to be reported. **Test:** Organizational processes for incident reporting; automated mechanisms supporting and/or implementing incident reporting.	

Table 152. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-6 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; information system design documentation; information system configuration settings and associated documentation; incident response plan; security plan; and other relevant documents or records. **Interview:** Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for incident reporting; automated mechanisms supporting and/or implementing reporting of security incidents.	

Table 153. 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.	
Guidance	
Possible incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii).	
Related Control Requirement(s):	AT-2, IR-4, IR-6, IR-8, SA-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-7 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records. **Interview:** Organizational personnel with incident response assistance and support responsibilities; organizational personnel with access to incident response support and assistance capability; organizational personnel with information security responsibilities. **Test:** Organizational processes for incident response assistance; automated mechanisms supporting and/or implementing incident response assistance.	

Table 154. 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.	
Guidance	
Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	

IR-7 (1): Automation Support for Availability of Information/Support
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the IR-7 (1) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records. **Interview:** Organizational personnel with incident response support and assistance responsibilities; organizational personnel with access to incident response support and assistance capability; organizational personnel with information security responsibilities. **Test:** Organizational processes for incident response assistance; automated mechanisms supporting and/or implementing an increase in the availability of incident response information and support.

Table 155. 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; 9. Is distributed to identified incident response personnel and organizational units, which may include: (i) Chief Information Security Officer; (ii) Chief Information Officer; (iii) Information System Security Officer; (iv) Attorney General/Computer Crimes Unit; (v) Personnel within the organization Incident Response Team; (vi) Personnel within the Personally Identifiable Information (PII) Breach Response Team; and (vii) Personnel within the organization Operations Centers; (viii) CMS b. Reviews within every three hundred sixty-five (365) days; c. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicates incident response plan changes to the organizational elements listed in 2(i) above; and e. Protects the incident response plan from unauthorized disclosure and modification.
Implementation Standards

IR-8: Incident Response Plan
1. The organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements for distribution of the response plan. The incident response list includes designated CMS personnel. 2. The organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements for communication of any changes. The incident response list includes designated CMS personnel. 3. Follow CMS guidance for Incident Handling, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .
Guidance
It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, Administering Entity organizations should coordinate and share IR information with external organizations, including, for example, external service providers and organizations involved in the support for organizational information systems and with whom the system has interconnections or information sharing. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(viii). CMS provides submission requirements and due dates for the Incident Response Plan in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sr/projects/cms_aca_program_security_privacy/ .
Related Control Requirement(s): MP-2, MP-4, MP-5
Control Implementation Description: The Incident Response Plan is a required artifact. "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the IR-8 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing incident response planning; incident response plan; records of incident response plan reviews and approvals; other relevant documents or records. **Interview:** Organizational personnel with incident response planning responsibilities; organizational personnel with information security responsibilities **Test:** Organizational incident response plan and related organizational processes.

Table 156. IR-9: Information Spillage Response

IR-9: Information Spillage Response
Control
The organization responds to information spills by: a. Requiring personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current Administering Entity (AE) organization Incident Handling Procedure and ACA incident handling reporting process available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ . b. Identifying the specific information involved in the improper or potentially improper information disclosure;

IR-9: Information Spillage Response	
c. Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill; d. Identifying other information systems or system components on which the information may have been subsequently improperly or potentially improperly shared with or disclosed to; and e. Removing and destroying the information from the contaminated information system, component or individual not authorized to handle the information.	
Guidance	
Information spillage in the context of the ACA program refers to instances where sensitive information [e.g., Personally Identifiable Information (PII) or infrastructure configurations] that is inadvertently placed on, subsequently shared with, or distributed to personnel or information systems that are not authorized to process such information. This would be considered an event that must be responded to per the requirements in IR-6. Such information spills may occur when information that is initially thought not to contain PII is transmitted to an information system or shared with an individual and then is subsequently determined to contain PII. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated systems. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination of the information.	
Related Control Requirement(s):	CP-4, IR-6, IR-8
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the IR-9 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Incident response policy; procedures addressing information spillage; incident response plan; records of information spillage alerts/notifications, list of personnel who should receive alerts of information spillage; list of actions to be performed regarding information spillage; other relevant documents or records. **Interview:** Organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for information spillage response; automated mechanisms supporting and/or implementing information spillage response actions and related communications.	

1.22 Maintenance (MA)

Table 157. MA-1: System Maintenance Policy and Procedures

MA-1: System Maintenance Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Maintenance (MA) family. Policy and procedures reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Maintenance policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with maintenance responsibilities; organizational personnel with information security responsibilities.	

Table 158. 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; 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;

MA-2: Controlled Maintenance	
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. **Implementation Standard(s)** 1. In facilities where Personally Identifiable Information (PII) is stored or accessed, document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).	
Guidance	
This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, and software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example, (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.	
Related Control Requirement(s):	CM-3, CM-4, MA-4, MP-6, PE-16, SI-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-2 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing controlled information system maintenance; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records. **Interview:** Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators. **Test:** Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the information system; organizational processes for sanitizing information system components; automated mechanisms supporting and/or implementing controlled maintenance; automated mechanisms implementing sanitization of information system components.	

Table 159. MA-3: Maintenance Tools

MA-3: Maintenance Tools
Control
The organization approves, controls, and monitors information system maintenance tools.
Guidance

MA-3: Maintenance Tools	
This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.	
Related Control Requirement(s):	MA-2, MA-5, MP-6
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-3 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing information system maintenance tools; information system maintenance tools and associated documentation; maintenance records; other relevant documents or records. **Interview:** Organizational personnel with information system maintenance responsibilities; and organizational personnel with information security responsibilities. **Test:** Organizational processes for approving, controlling, and monitoring maintenance tools; and automated mechanisms supporting and/or implementing approval, control, and/or monitoring of maintenance tools.	

Table 160. 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.	
Guidance	
If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.	
Related Control Requirement(s):	SI-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-3 (1) control as described in the control requirements.	

MA-3 (1): Inspect Tools
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing information system maintenance tools; information system maintenance tools and associated documentation; maintenance tool inspection records; maintenance records; other relevant documents or records. **Interview:** Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for inspecting maintenance tools; automated mechanisms supporting and/or implementing inspection of maintenance tools.

Table 161. 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.	
Guidance	
If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.	
Related Control Requirement(s):	SI-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-3 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing information system maintenance tools; information system maintenance tools and associated documentation; maintenance records; other relevant documents or records. **Interview:** Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational process for inspecting media for malicious code; automated mechanisms supporting and/or implementing inspection of media used for maintenance.	

Table 162. 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 information contained on the equipment;

MA-3 (3): Prevent Unauthorized Removal
b. Sanitizing or destroying the equipment; c. Retaining the equipment within the facility; or d. Obtaining an exemption, in writing, from the CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.
Guidance
Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the MA-3 (3) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing information system maintenance tools; information system maintenance tools and associated documentation; maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records. **Interview:** Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization. **Test:** Organizational process for preventing unauthorized removal of information; automated mechanisms supporting media sanitization or destruction of equipment; automated mechanisms supporting verification of media sanitization.

Table 163. 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 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 multi-factor authentication 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.
Guidance
Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA 2. Typically, strong authentication requires authenticators that are resistant to replay attacks

MA-4: Nonlocal Maintenance	
and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA 4 is accomplished in part by other controls.	
Related Control Requirement(s):	AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, SC-7, SC-10, SC-17
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-4 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing nonlocal information system maintenance; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; diagnostic records; other relevant documents or records. **Interview:** Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for managing nonlocal maintenance; automated mechanisms implementing, supporting, and/or managing nonlocal maintenance; automated mechanisms for strong authentication of nonlocal maintenance diagnostic sessions; automated mechanisms for terminating nonlocal maintenance sessions and network connections.	

Table 164. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-4 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing nonlocal information system maintenance; list of audit events; information system configuration settings and associated documentation; maintenance records; diagnostic records; audit records; reviews of maintenance and diagnostic session records; other relevant documents or records.	

MA-4 (1): Auditing and Review
Interview: Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel with audit and review responsibilities; system/network administration.

Table 165. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-4 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing non-local information system maintenance; security plan; maintenance records; diagnostic records; audit records; other relevant documents or records. **Interview:** Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities.	

Table 166. MA-4 (3): Comparable Security/Sanitization

MA-4 (3): Comparable Security/Sanitization
Control
The organization: a. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system serviced; or b. Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.
Guidance
Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system serviced.

MA-4 (3): Comparable Security/Sanitization	
Related Control Requirement(s):	MA-3, SI-3, SI-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MA-4 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system maintenance policy; procedures addressing nonlocal information system maintenance; service provider contracts and/or service level agreements; maintenance records; inspection records; audit records; equipment sanitization records; media sanitization records; other relevant documents or records. **Interview:** Organizational personnel with information system maintenance responsibilities; information system maintenance provider; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators. **Test:** Organizational processes for comparable security and sanitization for nonlocal maintenance; organizational processes for removal, sanitization, and inspection of components services via nonlocal maintenance; automated mechanisms supporting and/or implementing component sanitization and inspection.	

Table 167. 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; 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.
Guidance
This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, system integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

MA-5: Maintenance Personnel	
Related Control Requirement(s):	AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the MA-5 control as described in the control requirements.

Assessment Methods and Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts; service level agreements; list of authorized personnel; maintenance records; access control records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for authorizing and managing maintenance personnel; automated mechanisms supporting and/or implementing authorization of maintenance personnel.

Table 168. 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.	
Guidance	
Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.	
Related Control Requirement(s):	CM-8, CP-2, CP-7

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the MA-6 control as described in the control requirements.

Assessment Methods and Objects

Examine: Information system maintenance policy; procedures addressing information system maintenance; service provider contracts; service level agreements; inventory and availability of spare parts; security plan; other relevant documents or records.

MA-6: Timely Maintenance
Interview: Organizational personnel with information system maintenance responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for ensuring timely maintenance.

1.23 Media Protection (MP)

Table 169. MP-1: Media Protection Policy and Procedures

MP-1: Media Protection Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable) ,within every three hundred sixty-five (365) days: a. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the media protection policy and associated media protection controls. **Implementation Standards** 1. Semi-annual inventories of removable media containing Personally Identifiable Information (PII) are conducted. The organization accounts for any missing removal media containing PII by documenting the search efforts and notifying the media initiator of the loss. 2. Information system media includes both digital media (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).	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Media Protection (MP) family. Policy and procedures reflect applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-1 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Media protection policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with information system media protection responsibilities; organizational personnel with information security responsibilities.	

Table 170. 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.	
Guidance	
Information system media includes both digital media (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 and microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.	
Related Control Requirement(s):	AC-3, IA-2, MP-4, PE-2, PE-3
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-2 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system media protection policy; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records. **Interview:** Organizational personnel with information system media protection responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for restricting information media; automated mechanisms supporting and/or implementing media access restrictions.	

Table 171. 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. Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the media remain within a secure environment.
Guidance
The term *marking* is used when referring to the application or use of human-readable security attributes. The term *labeling* is used when referring to the application or use of security attributes with regard to internal data structures

MP-3: Media Marking	
within the information system. Removable information system media includes both digital media (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 and microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Organizations may extend the scope of this control to include information system output devices containing sensitive information (such as Personally Identifiable Information), including, for example, monitors and printers.	
Related Control Requirement(s):	RA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-3 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; list of information system media marking security attributes; designated controlled areas; other relevant documents or records. **Interview:** Organizational personnel with information system media protection and marking responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for marking information media; automated mechanisms supporting and/or implementing media marking.	

Table 172. 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 Personally Identifiable Information (PII) is recorded on magnetic media with other data, it should be protected as if it were entirely PII.
Guidance
Information system media includes both digital media (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 and microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting information and/or information system.

MP-4: Media Storage	
An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. As part of a defense-in-depth strategy, the organization considers routinely encrypting sensitive information at rest on selected secondary storage devices. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information.	
Related Control Requirement(s):	CP-6, CP-9, MP-2, MP-7, PE-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-4 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media; designated controlled areas; other relevant documents or records. **Interview:** Organizational personnel with information system media protection and storage responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for storing information media; automated mechanisms supporting and/or implementing secure media storage/media protection.	

Table 173. MP-5: Media Transport

MP-5: Media Transport
Control
The organization: a. Protects and controls digital and non-digital media containing sensitive information, such as Personally Identifiable Information (PII), during transport outside of controlled areas using cryptography and tamper-evident packaging, and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) 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. **Implementation Standards** 1. Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit. 2. The organization protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas, and encrypts digital media via a FIPS 140-2 validated encryption module.

MP-5: Media Transport	
3. The organization defines security measures to protect digital and non-digital media in transport.	
Guidance	
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-5 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with information system media transport responsibilities; organizational personnel with information security responsibilities; system/network administrators]. **Test:** Organizational processes for transporting media; automated mechanisms supporting and/or implementing media transport.	

Table 174. 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.	
Guidance	
This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, and external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, and E-readers).	
Related Control Requirement(s):	MP-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-5 (4) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system media protection policy; procedures addressing media transport; information system design documentation; information system configuration settings and associated documentation; information system media transport records; audit records; other relevant documents or records **Interview:** Organizational personnel with information system media transport responsibilities; organizational personnel with information security responsibilities. **Test:** Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas.	

Table 175. 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 applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. **Implementation Standard(s)** 1. Employ sanitization mechanisms consistent with guidance provided in NIST Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization*. 2. Finely shred hard-copy documents using approved equipment, techniques, and procedures, and with a minimum of cross-cut shredding. 3. Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability.

MP-6: Media Sanitization
Tapes containing Personally Identified Information, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies: a. Date received; b. Reel/cartridge control number contents; c. Number of records, if available; d. Movement; and e. If disposed of, the date and method of disposition. 4. Surplus equipment is stored securely while not in use, and disposed of or sanitized in accordance with NIST SP 800-88 Revision 1 when no longer required.
Guidance
This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, and prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal.
Related Control Requirement(s): MA-2, MA-4, RA-3, SC-4
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the MP-6 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; applicable standards and policies addressing media sanitization; media sanitization records; audit records; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** Organizational personnel with information system media sanitization responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for media sanitization; automated mechanisms supporting and/or implementing media sanitization.

Table 176. MP-6 (1): Review/Approve/Track/Document/Verify

MP-6 (1): Review/Approve/Track/Document/Verify
Control
The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions. **Implementation Standards**

MP-6 (1): Review/Approve/Track/Document/Verify	
The organization ensures Personally Identifiable Information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.	
Guidance	
Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(4)(vi).	
Related Control Requirement(s):	SI-12
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-6 (1) control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Information system media protection; procedures addressing media sanitization and disposal; media sanitization and disposal records; review records for media sanitization and disposal actions; approvals for media sanitization and disposal actions; tracking records; verification records; audit records; other relevant documents or records. **Interview:** Organizational personnel with information system media sanitization and disposal responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for media sanitization; automated mechanisms supporting and/or implementing the review/approval/track/document/verify of media sanitization.	

Table 177. MP-6 (2): Equipment Testing

MP-6 (2): Equipment Testing – Enhancement	
Control	
The organization tests sanitization equipment and procedures within every three hundred sixty-five (365) days to verify that the equipment is achieving the intended sanitization.	
Guidance	
Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	

MP-6 (2): Equipment Testing – Enhancement
Assessment Objective Determine if the organization has implemented all elements of the MP-6 (2) control as described in the control requirements.
Assessment Methods and Objects **Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; procedures addressing testing of media sanitization equipment; results of media sanitization equipment and procedures testing; audit records; other relevant documents or records. **Interview:** Organizational personnel with information system media sanitization responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for media sanitization; automated mechanisms supporting and/or implementing media sanitization equipment testing.

Table 178. MP-7: Media Use

MP-7: Media Use	
Control	
The organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).	
Guidance	
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, and E-readers). In contrast to MP 2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, and rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.	
Related Control Requirement(s):	AC-19, PL-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-7 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system media protection policy; system use policy; procedures addressing media usage restrictions; security plan; rules of behavior; information system design documentation; information system configuration settings and associated documentation; audit records; other relevant documents or records,	

MP-7: Media Use
Interview: Organizational personnel with information system media use responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for media use; automated mechanisms restricting or prohibiting use of information system media on information systems or system components.

Table 179. 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.	
Guidance	
Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).	
Related Control Requirement(s):	PL-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-7 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system media protection policy; system use policy; procedures addressing media usage restrictions; security plan; rules of behavior; information system design documentation; information system configuration settings and associated documentation; audit records; other relevant documents or records. **Interview:** Organizational personnel with information system media responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for media use; automated mechanisms restricting or prohibiting use of information system media on information systems or system components.	

Table 180. MP-CMS-1: Media Related Records

MP-CMS-1: Media Related Records
Control
Inventory and disposition records for information system media shall be maintained to ensure control and accountability of sensitive information. The media-related records shall contain sufficient information to reconstruct the data in the event of a breach. **Implementation Standards**

MP-CMS-1: Media Related Records	
1. The media records must, at a minimum, contain: a. The name of media recipient; b. Signature of media recipient; c. Date/time media received; d. Media control number and contents; e. Movement or routing information; and f. If disposed of, the date, time, and method of destruction.	
Guidance	
The organization employs a hash function (a reproducible method of turning inventory data into a relatively small number, which may serve as a digital "fingerprint" of the data) for electronic inventory records maintenance to validate, during investigation of a possible breach, whether the inventory information is free from tampering prior to reconstructive events.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the MP-CMS-1 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Media protection policy and procedures; procedures addressing media record keeping; records of media accounting; audit records; other relevant documents or records. **Interview:** Organizational personnel with information system media protection responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for media record keeping; automated mechanisms supporting and/or implementing media record keeping.	

1.24 Physical and Environmental Protection (PE)

Table 181. PE-1: Physical and Environmental Protection Policy and Procedures

PE-1: Physical and Environmental Protection Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A formal documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Physical and Environmental Protection (PE) family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with physical and environmental protection responsibilities; organizational personnel with information security responsibilities.	

Table 182. 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; and

PE-2: Physical Access Authorizations
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.
Guidance
This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.
Related Control Requirement(s): PE-3, PE-4, PS-3
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the PE-2 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; physical access list reviews; physical access termination records and associated documentation; other relevant documents or records. **Examine:** Restricted areas, security rooms, or locked rooms that control access to areas containing PII. **Interview:** Organization personnel responsible for controlling restricted areas including security rooms, or locked rooms containing PII; organizational personnel with physical access to information system facility; organizational personnel with information security responsibilities. **Test:** Organizational processes for physical access authorizations; automated mechanisms supporting and/or implementing physical access authorizations.

Table 183. 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 and information is received, processed, stored, or transmitted based on position or role.
Guidance
Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where information is received, processed, stored, or transmitted.

PE-2 (1): Access by Position / Role	
Related Control Requirement(s):	AC-2, AC-3, AC-6

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PE-2 (1) control as described in the control requirements.

Assessment Methods and Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; physical access control logs or records; list of positions/roles and corresponding physical access authorizations; information system entry and exit points; other relevant documents or records.

Examine: Restricted areas, security rooms, or locked rooms that control access to areas containing Personally Identifiable Information (PII).

Interview: Organization personnel responsible for controlling restricted areas, security rooms, or locked rooms; organizational personnel with physical access to information system facility; organizational personnel with information security responsibilities.

Test: Organizational processes for physical access authorizations; automated mechanisms supporting and/or implementing physical access authorizations.

Table 184. PE-3: Physical Access Control

PE-3: Physical Access Control
Control

The organization:

a. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible;
b. Escorts visitors and monitors visitor activity;
c. Enforces physical access authorizations at defined entry/exit points to the facility (defined in the applicable security plan) where the information system resides;
d. Verifies individual access authorizations before granting access to the facility;
e. Controls entry to the facility containing the information system using physical access devices/or guards;
f. Maintains physical access audit logs for defined entry/exit points;
g. Secures keys, combinations, and other physical access devices;
h. Inventories physical access devices within every three hundred sixty-five (365) days: and
i. 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.

PE-3: Physical Access Control	
Protected information must be containerized in areas where other than authorized employees may have access afterhours. 5. Escort and monitor visitor activity.	
Guidance	
This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-3 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; information system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records. **Examine:** Protection barriers. **Interview:** Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for physical access control; automated mechanisms supporting and/or implementing physical access control; physical access control devices.	

Table 185. 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 Standards** 1. Disable any physical ports (e.g., wiring closets and patch panels) not in use.

PE-4: Access Control for Transmission Medium	
Guidance	
Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in-transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example, (i) locked wiring closets; (ii) disconnected or locked spare jacks, and/or (iii) protection of cabling by conduit or cable trays.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-4 control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; list of physical security safeguards applied to information system distribution and transmission lines; other relevant documents or records; facility communications and wiring diagrams; telecommunications/wiring closets. **Interview:** Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for access control to distribution and transmission lines; automated mechanisms/security safeguards supporting and/or implementing access control to distribution and transmission lines.	

Table 186. 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.	
Guidance	
Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.	
Related Control Requirement(s):	PE-2, PE- 3, PE-4, PE-18, SC-ACA-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective	

PE-5: Access Control for Output Devices
Determine if the organization has implemented all elements of the PE-5 control as described in the control requirements.
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; actual displays from information system components; other relevant documents or records. **Interview:** Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for access control to output devices; automated mechanisms supporting and/or implementing access control to output devices.

Table 187. 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 weekly 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 Standards** 1. The organization reviews physical access logs at least every two (2) months.	
Guidance	
Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example, (i) accesses outside of normal work hours, (ii) repeated accesses to areas not normally accessed, (iii) accesses for unusual lengths of time, and (iv) out-of-sequence accesses.	
Related Control Requirement(s):	CA-7, IR-4, IR-8
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-6 control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical access logs or records; physical access monitoring records; physical access log reviews; other relevant documents or records. **Interview:** Organizational personnel with physical access monitoring responsibilities; organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities.	

PE-6: Monitoring Physical Access
Test: Organizational processes for monitoring physical access; automated mechanisms supporting and/or implementing physical access monitoring; automated mechanisms supporting and/or implementing reviewing of physical access logs.

Table 188. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-6 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; physical access monitoring records; physical access log reviews; other relevant documents or records. **Interview:** Organizational personnel with physical access monitoring responsibilities; organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for monitoring physical intrusion alarms and surveillance equipment; automated mechanisms supporting and/or implementing physical access monitoring; automated mechanisms supporting and/or implementing physical intrusion alarms and surveillance equipment.	

Table 189. 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.	
Guidance	
Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	

PE-8: Visitor Access Records
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the PE-8 control as described in the control requirements.
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control logs or records; visitor access record or log reviews; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for reviewing visitor physical access records; organizational personnel with information security responsibilities. **Test:** Organizational processes for maintaining and reviewing visitor access records; automated mechanisms supporting and/or implementing maintenance and review of visitor access records.

Table 190. PE-9: Power Equipment and Cabling

PE-9: Power Equipment and Cabling	
Control	
The organization protects power equipment and power cabling for the information system from damage and destruction. **Implementation Standards** 1. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.	
Guidance	
Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.	
Related Control Requirement(s):	PE-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-9 control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records. **Interview:** Organizational personnel with responsibility for protecting power equipment/cabling; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing protection of power equipment/cabling.	

Table 191. PE-10: Emergency Shutoff

PE-10: Emergency Shutoff	
Control	
The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	
Guidance	
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.	
Related Control Requirement(s):	PE-15
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-10 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; locations housing emergency shutoff switches and devices; security safeguards protecting emergency power shutoff capability from unauthorized activation; other relevant documents or records. **Interview:** Organizational personnel with responsibility for emergency power shutoff capability (both implementing and using the capability); organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing emergency power shutoff.	

Table 192. PE-11: Emergency Power

PE-11: Emergency Power	
Control	
The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	
Related Control Requirement(s):	AT-3, CP-2, CP-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-11 control as described in the control requirements.	

PE-11: Emergency Power
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; other relevant documents or records. **Interview:** Organizational personnel with responsibility for emergency power and/or planning; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing uninterruptible power supply; the uninterruptable power supply.

Table 193. PE-12: Emergency Lighting

PE-12: Emergency Lighting	
Control	
The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.	
Guidance	
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.	
Related Control Requirement(s):	CP-2, CP-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-12 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; areas/locations within facility supporting essential missions and business functions; other relevant documents or records. **Interview:** Organizational personnel with emergency lightning and/or planning responsibilities; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing emergency lighting capability.	

Table 194. PE-13: Fire Protection

PE-13: Fire Protection
Control
The organization employs and maintains for the information system fire suppression and detection devices/systems supported by an independent energy source.
Guidance
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection

PE-13: Fire Protection	
devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-13 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; disaster recovery plan; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records; fire extinguisher charged? **Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing fire suppression/detection devices/systems.	

Table 195. PE-13 (1): Detection Devices/Systems

PE-13 (1): Detection Devices/Systems	
Control	
The organization employs fire detection devices/systems for the information system that activate automatically and notify defined personnel or roles (defined in the applicable security plan) and defined emergency responders (defined in the applicable security plan) in the event of a fire.	
Guidance	
Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-13 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection	

PE-13 (1): Detection Devices/Systems
devices/systems; fire suppression and detection devices/systems documentation; alerts/notifications of fire events; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with responsibilities for notifying appropriate personnel, roles, and emergency responders of fires; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing fire detection devices/systems; activation of fire detection devices/systems (simulated); automated notifications.

Table 196. PE-13 (2): Suppression Devices/Systems

PE-13 (2): Suppression Devices/Systems	
Control	
The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to defined personnel (or roles) and defined emergency responders.	
Guidance	
Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-13 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with responsibilities for providing automatic notifications of any activation of fire suppression devices/systems to appropriate personnel, roles, and emergency responders; organizational personnel with information security responsibilities. Test**:** Automated mechanisms supporting and/or implementing fire suppression devices/systems; activation of fire suppression devices/systems (simulated); automated notifications.	

Table 197. PE-13 (3): Automatic Fire Suppression

PE-13 (3): Automatic Fire Suppression
Control
The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

PE-13 (3): Automatic Fire Suppression	
Related Control Requirement(s):	

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PE-13 (3) control as described in the control requirements.

Assessment Methods and Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; other relevant documents or records.

Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with responsibilities for providing automatic notifications of any activation of fire suppression devices/systems to appropriate personnel, roles, and emergency responders; organizational personnel with information security responsibilities.

Test: Automated mechanisms supporting and/or implementing fire suppression devices/systems; activation of fire suppression devices/systems (simulated).

Table 198. PE-14: Temperature and Humidity Controls

PE-14: Temperature and Humidity Controls	

Control

The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and

b. Monitors temperature and humidity levels.

Implementation Standards

1. Evaluate the level of alert and follow prescribed guidelines for that alert level.
2. Alert component management of possible loss of service and/or media.
3. Report damage and provide remedial action. Implement contingency plan, if necessary.

Guidance

This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

Related Control Requirement(s):	AT-3

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PE-14 control as described in the control requirements and associated implementation standards.

PE-14: Temperature and Humidity Controls
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing temperature and humidity control; security plan; temperature and humidity controls; disaster recovery plans; facility housing the information system; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records; telecommunications/wiring closets. **Interview:** Organizational personnel with responsibilities for information system environmental controls; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing maintenance and monitoring of temperature and humidity levels including alert levels.

Table 199. PE-15: Water Damage Protection

PE-15: Water Damage Protection	
Control	
The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	
Guidance	
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.	
Related Control Requirement(s):	AT-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-15 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; location of master shutoff valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; other relevant documents or records. **Interview:** Organization personnel with physical and environmental protection responsibilities; organizational personnel with information security responsibilities. **Test:** Master water-shutoff valves; organizational process for activating master water-shutoff.	

Table 200. PE-16: Delivery and Removal

PE-16: Delivery and Removal
Control
The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items.

PE-16: Delivery and Removal	
Implementation Standards 1. The organization authorizes, monitors, and controls the flow of all information system components entering and exiting the facility and maintains records of those items.	
Guidance	
Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.	
Related Control Requirement(s):	CM-3, MA-2, MA-3, MP-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PE-16 control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; disaster recovery plan; security plan; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records. **Interview:** Organization personnel with responsibilities for controlling information system components entering and exiting the facility; organizational personnel with information security responsibilities. **Test:** Organizational process for authorizing, monitoring, and controlling information system-related items entering and exiting the facility; automated mechanisms supporting and/or implementing authorizing, monitoring, and controlling information system-related items entering and exiting the facility.	

Table 201. PE-17: Alternate Work Site

PE-17: Alternate Work Site
Control
The organization: a. Employs appropriate security controls at alternate work sites that include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. **Implementation Standards** 2. The organization defines management, operational, and technical information system security controls for alternate work sites.
Guidance
Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

PE-17: Alternate Work Site	
Related Control Requirement(s):	AC-17, CP-7

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PE-17 control as described in the control requirements and associated implementation standard.

Assessment Methods and Objects

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; security plan; list of management, operational, and technical security controls required for alternate work sites; assessments of security controls at alternate work sites; other relevant documents or records.

Interview: Organizational personnel approving use of alternate work sites; organizational personnel using alternate work sites; organizational personnel assessing controls at alternate work sites; organizational personnel with information security responsibilities.

Test: Organizational processes for security at alternate work sites; automated mechanisms supporting alternate work sites; security controls employed at alternate work sites; means of communications between personnel at alternate work sites and security personnel.

Table 202. PE-18: Location of Information System Components

PE-18: Location of Information System Components	
Control	
The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.	
Guidance	
Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).	
Related Control Requirement(s):	CP-2, RA-3

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PE-18 control as described in the control requirements.

Assessment Methods and Objects

Examine: Physical and environmental protection policy; procedures addressing positioning of information system components; disaster recovery plans; documentation providing the location and position of information system

PE-18: Location of Information System Components
components within the facility; locations housing information system components within the facility; list of physical and environmental hazards with potential to damage information system components within the facility; other relevant documents or records. **Interview:** Organizational personnel with responsibilities for positioning information system components; organizational personnel with information security responsibilities. **Test:** Organizational processes for positioning information system components.

1.25 Planning (PL)

Table 203. PL-1: Security Planning Policy and Procedures

PL-1: Security Planning Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the security planning policy and associated security planning controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Planning (PL) family. Policy and procedures reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The security planning procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PL-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Security planning policy and procedures; and other relevant documents or records. **Interview:** Organizational personnel with planning responsibilities; organizational personnel with security planning responsibilities.	

Table 204. 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 the ACA System Security Plan (SSP) Procedure; 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;

PL-2: System Security Plan

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. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. 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.

Implementation Standards

When developing new system security plans or updating prior system security plans use the *System Security Plan Template for ACA Administering Entity Systems,* which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .

Guidance

Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the ACA program if the plan is implemented as intended.

Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information, but instead provide, explicitly or by reference, sufficient information to define what those plans must accomplished.

All ACA information systems and major applications are covered by a SSP that is compliant with current ACA SSP Procedures.

CMS provides submission requirements and due dates for the SSP in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ . Detailed instructions for completing the SSP are contained in Volume IV of the MARS-E document suite,

Related Control Requirement(s):	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, PM-1, PM-8, PM-9, PM-11, SA-5

Control Implementation Description:

*** Note: The System Security Plan (SSP) is a required artifact.

"Click here and type text"

PL-2: System Security Plan
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the PL-2 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates; and other relevant documents or records. (For Personally Identifiable Information only) Procedures that specify who obtains documentation and which documentation pertains to whom for implementation. **Interview:** Organization personnel with security planning and plan implementation; organizational personnel with information security responsibilities organizational personnel who are responsible for implementation of procedures to determine if documentation is available. **Test:** Organizational processes for security plan development/review/update/approval; automated mechanisms supporting the information system security plan.

Table 205. 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.	
Guidance	
Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or not urgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate.	
Related Control Requirement(s):	CP-4, IR-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PL-2 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Security planning policy; access control policy; contingency planning policy; procedures addressing security-related activity planning for the information system; security plan for the information system; contingency plan for the information system; information system design documentation; other relevant documents or records **Interview:** Organization personnel with security planning and plan implementation responsibilities; organizational individuals or groups with whom security-related activities are to be planned and coordinated; organizational personnel with information security responsibilities	

Table 206. 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. **Implementation Standards** Rules of behavior are aligned with DHHS requirements posted at: http://www.hhs.gov/ocio/policy/hhs-rob.html .	
Guidance	
This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from the ACA system, is often not feasible given the large number of these users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b, the acknowledgment portion of this control, may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures (or other electronic mechanisms) for acknowledging 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, MP-7, PS-6, PS-8, SA-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PL-4 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; signed acknowledgements; records for rules of behavior reviews and updates; other relevant documents or records. **Interview:** Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel who are authorized users of the information system and have signed and resigned rules of behavior; organizational personnel with information security responsibilities. **Test:** Organizational processes for establishing, reviewing, disseminating, and updating rules of behavior; automated mechanisms supporting and/or implementing the establishment, review, dissemination, and update of rules of behavior.	

Table 207. 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.	
Guidance	
This control enhancement addresses rules of behavior related to the use of social media/networking sites (i) when organizational personnel are using such sites for official duties or in the conduct of official business, (ii) when organizational information is involved in social media/networking transactions, and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information and personally identifiable information) from social media/networking sites.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PL-4 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; and other relevant documents or records. **Interview:** Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel who are authorized users of the information system and have signed rules of behavior; organizational personnel with information security responsibilities. **Test:** Organizational processes for establishing rules of behavior; automated mechanisms supporting and/or implementing the establishment of rules of behavior.	

Table 208. 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.
Guidance

PL-8: Information Security Architecture	
This control addresses actions taken by organizations in the design and development of ACA systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role; unique security requirements; the types of information processed, stored, and transmitted by the information system; restoration priorities of information and information system services; and any other specific protection needs. There are key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive ACA system protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the senior Administering Entity privacy officer to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the ACA system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture.	
Related Control Requirement(s):	CM-2, CM-6, PL-2, PM-7, SA-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PL-8 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Security planning policy; procedures addressing information security architecture development; procedures addressing information security architecture reviews and updates; enterprise architecture documentation; network architecture diagram; information security architecture documentation; security plan for the information system; security CONOPS for the information system; records of information security architecture reviews and updates; other relevant documents or records. **Interview:** Organizational personnel with security planning and plan implementation responsibilities; organizational personnel with information security architecture development responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for developing, reviewing, and updating the information security architecture; automated mechanisms supporting and/or implementing the development, review, and update of the information security architecture.	

1.26 Personnel Security (PS)

Table 209. PS-1: Personnel Security Policy and Procedures

PS-1: Personnel Security Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Personnel Security (PS) family. Policy and procedures reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (c).	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PS-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Personnel security policy and procedures; and other relevant documents or records. **Interview:** Organizational personnel access control responsibilities; and organizational personnel with information security responsibilities.	

Table 210. 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 hundred sixty-five (365) days.

PS-2: Position Risk Designation	
Guidance	
Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training and security clearances). This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (c).	
Related Control Requirement(s):	AT-3, PL-2, PS-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PS-2 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; security plan; records of position risk designation reviews and updates; and other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities; and organizational personnel with information security responsibilities. **Test:** Organizational processes for assigning, reviewing, and updating position risk designations; and organizational processes for establishing screening criteria.	

Table 211. 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 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.
Guidance
Personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

PS-3: Personnel Screening	
Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.	
Related Control Requirement(s):	AC-2, IA-4. PE-2, PS-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PS-3 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; and other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities; and organizational personnel with information security responsibilities. **Test:** Organizational processes for personnel screening.	

Table 212. 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).
Guidance
Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed on former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In

PS-4: Personnel Termination	
certain situations, organizations consider disabling the information system accounts of individuals who are being terminated prior to notifying the individuals of their termination. Appropriate personnel have access to official records created by terminated employees that are stored on information systems.	
Related Control Requirement(s):	AC-2, IA-4, PE-2, PS-5, PS-6
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PS-4 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; records of terminated or revoked authenticators/credentials; records of exit interviews; other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities; organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities. **Test:** Organizational processes for personnel termination; automated mechanisms supporting and/or implementing personnel termination notifications; and automated mechanisms for disabling information system access/revoking authenticators.	

Table 213. 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 as soon as possible but not to exceed thirty (30) days; 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.
Guidance
This control applies when reassignments or transfers of individuals are permanent or of such extended durations to warrant action. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example, (i) returning old and issuing new keys, identification cards, and building

PS-5: Personnel Transfer	
passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.	
Related Control Requirement(s):	AC-2, IA-4, PE-2, PS-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PS-5 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; and other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities; organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities. **Test:** Organizational processes for personnel transfer; automated mechanisms supporting and/or implementing personnel transfer notifications; automated mechanisms for disabling information system access/revoking authenticators.	

Table 214. 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.
Guidance
Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. This control supports and aligns 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).

PS-6: Access Agreements	
Related Control Requirement(s):	PL-4, PS-2, PS-3, PS-4, PS-8

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PS-6 control as described in the control requirements.

Assessment Methods and Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; organizational personnel who have signed/resigned access agreements; organizational personnel with information security responsibilities.

Test: Organizational processes for access agreements; automated mechanisms supporting access agreements.

Table 215. 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 fifteen (15) calendar days; and

e. Monitors provider compliance.

Implementation Standards

1. 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.

Guidance

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.

PS-7: Third-Party Personnel Security	
Related Control Requirement(s):	PS-2, PS-3, PS-4, PS-5, PS-6, SA-9

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PS-7 control as described in the control requirements and associated implementation standards.

Assessment Methods and Objects

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; service-level agreements; compliance monitoring process; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; third-party providers; system/network administrators; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for managing and monitoring third-party personnel security; automated mechanisms supporting and/or implementing monitoring of provider compliance.

Table 216. 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) when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
Guidance
Organizational sanctions processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (c) and (g). Since the FFM is a federal collection of Personally Identifiable Information (PII) and the Privacy Act applies, employees, contractors and agents are obligated to comply with the Supplemental Standards of Ethical Conduct for Employees of the Department of Health and Human Services and with the HHS Residual Standards of Conduct. All employees must guard against improper disclosure of records, which are governed by the Privacy Act. Because of the serious consequences of improper invasions of personal privacy, employees may be subject to disciplinary action and criminal prosecution for knowing and willful violations of the Act and regulation. In addition, employees may also be subject to disciplinary action for unknowing or unwillful violations, where the employee had notice of the provisions of the Act and regulations and failed to inform himself sufficiently or to conduct himself in accordance with the requirements to avoid violations.

PS-8: Personnel Sanctions	
Related Control Requirement(s):	PL-4, PS-6

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PS-8 control as described in the control requirements.

Assessment Methods and Objects

Examine: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities.

Test: Organizational processes for managing personnel sanctions; automated mechanisms supporting and/or implementing notifications.

1.27 Risk Assessment (RA)

Table 217. RA-1: Risk Assessment Policy and Procedure

RA-1: Risk Assessment Policy and Procedure	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable) within every three hundred sixty-five (365) days: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Risk Assessment (RA) family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the RA-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Risk assessment policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with risk assessment responsibilities; organizational personnel with information security responsibilities.	

Table 218. RA-2: Security Categorization

RA-2: Security Categorization
Control
The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-2: Security Categorization	
Guidance	
Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. All information systems categorized as High or Moderate are considered sensitive or to contain sensitive information. All information systems categorized as Low are considered non-sensitive or to contain non-sensitive information. The requirements contained in this CMS *Catalog of Security and Privacy Controls for Exchanges* are for CMS's minimum acceptable risk standards for systems categorized as Moderate.	
Related Control Requirement(s):	CM-8, MP-4, RA-3, SC-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the RA-2 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Risk assessment policy; security planning policy and procedures; procedures addressing security categorization of organizational information and information systems; security plan; security categorization documentation; other relevant documents or records. **Interview:** Organizational personnel with security categorization and risk assessment responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for security categorization	

Table 219. 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, Business Owners(s), and CMS; 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. (Significant change is defined in NIST Special Publication 800 37 Revision 1, Section F.4 of Appendix F.) **Implementation Standards**

RA-3: Risk Assessment
1. The organization conducts an information security risk assessment and documents risk assessment results in the security assessment report template that can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ . 2. The system owner reviews risk assessment results at least every three hundred sixty-five (365) days or when a significant change occurs.
Guidance
Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., entities with whom the organization has established data sharing arrangements, service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, and outsourcing entities). Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework (reference NIST Special Publication 800-37 Revision 1, *Guide for applying the Risk Management Framework to Federal Information Systems*), including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy because the control must be partially implemented prior to the implementation of other controls to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs (a)(3)(viii), and (a)(4)(iv). CMS provides submission requirements and due dates for the Risk Assessment in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .
Related Control Requirement(s): PM-9, RA-2
Control Implementation Description: ***The Information Security Risk Assessment (ISRA) is a required artifact. "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the RA-3 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records. **Interview:** Organizational personnel with risk assessment responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for risk assessment; automated mechanisms supporting and/or for conducting, documenting, reviewing, disseminating, and updating the risk assessment.

Table 220. 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 vulnerabilities potentially affecting the system/applications are identified and reported; 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** 3. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with organizational Information Security procedures. 4. Legitimate high-risk vulnerabilities are mitigated within thirty (30) days, and moderate risk vulnerabilities are mitigated within ninety (90) days.	
Guidance	
Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, and binary analyzers) and in source code reviews. Vulnerability scanning includes, for example, (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments, such as red team exercises, provide other sources of potential vulnerabilities for scanning. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).	
Related Control Requirement(s):	CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the RA-5 control as described in the control requirements and associated implementation standards.	

RA-5: Vulnerability Scanning
Assessment Methods and Objects **Examine:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; penetration testing results; patch and vulnerability management records; other relevant documents or records. **Interview:** Organizational personnel with risk assessment, security control assessment, and vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with vulnerability remediation and vulnerability scanning responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing. Automated mechanisms implementing the requirement to perform external penetration testing.

Table 221. 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.	
Guidance	
The vulnerability scanning tools must be capable of full updating as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.	
Related Control Requirement(s):	SI-3, SI-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the RA-5 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Procedures addressing vulnerability scanning; security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; risk assessment policy; other relevant documents or records. **Interview:** Organizational personnel with vulnerability scanning responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning.	

Table 222. 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 or when new vulnerabilities are identified and reported.	
Related Control Requirement(s):	SI-3, SI-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the RA-5 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Procedures addressing vulnerability scanning; security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; risk assessment policy; other relevant documents or records. **Interview:** Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning.	

Table 223. RA-5 (3): Breadth/Depth of Coverage

RA-5 (3): Breadth/Depth of Coverage	
Control	
The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the RA-5 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Risk assessment policy; procedures addressing vulnerability scanning; security plan; risk assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records. **Interview:** Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with information security responsibilities.	

RA-5 (3): Breadth/Depth of Coverage
Test: Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning.

Table 224. 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.	
Guidance	
In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the RA-5 (5) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Risk assessment policy; procedures addressing vulnerability scanning; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; other relevant documents or records. **Interview:** Organizational personnel with vulnerability scanning responsibilities; system/network administrators; organizational personnel responsible for access control to the information system; system developers; organizational personnel with information security responsibilities. **Test:** Organizational processes for vulnerability scanning; organizational processes for access control; automated mechanisms supporting and/or implementing access control; automated mechanisms/tools supporting and/or implementing vulnerability scanning.	

1.28 System and Services Acquisition (SA)

Table 225. SA-1: System and Services Acquisition Policy and Procedures

SA-1: System and Services Acquisition Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable), within every three hundred sixty-five (365) days: a. A formal documented system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the System and Services Acquisition (SA) family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities	

Table 226. 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; c. Includes information security requirements in mission/business case planning, and

SA-2: Allocation of Resources	
d. Establishes a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.	
Guidance	
Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.	
Related Control Requirement(s):	PM-3, PM-11
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-2 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; procedures addressing capital planning and investment control; organizational programming and budgeting documentation; other relevant documents or records. **Interview:** Organizational personnel with capital planning and investment control, organizational programming and budgeting responsibilities; organizational personnel responsible for determining information security requirements for information systems/services; organizational personnel with information security responsibilities. **Test:** Organizational processes for determining information security requirements; organizational processes for capital planning, programming, and budgeting; automated mechanisms supporting and/or implementing organizational capital planning, programming, and budgeting.	

Table 227. 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.
Guidance
A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals who design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers, in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on

SA-3: System Development Life Cycle	
the development team who possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. CMS provides submission requirements and due dates for documentation required during the systems development life cycle for Administering Entity IT systems in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
Related Control Requirement(s):	AT-3, PM-7, SA-8, AR-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-3 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; information system development life cycle documentation; information security risk management strategy/program documentation; other relevant documents or records. **Interview:** Organizational personnel with information security and system life cycle development responsibilities; organizational personnel with information security risk management responsibilities; business and/or system owners; system developers; organizational personnel with information security responsibilities. **Test:** Organizational processes for defining and documenting the SDLC; organizational processes for identifying SDLC roles and responsibilities; organizational process for integrating information security risk management into the SDLC; automated mechanisms supporting and/or implementing the SDLC.	

Table 228. SA-4: Acquisition Process

SA-4: Acquisition Process
Control
The organization 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: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate;

SA-4: Acquisition Process
g. Acceptance criteria; and h. Requirement that providers of defined external information systems identify the location of information systems that receive, process, store, or transmit data. **Implementation Standards** 1. Each contract and Statement of Work (SOW) that requires development or access to systems that contain Personally Identifiable Information (PII) must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR §155.260(b); define security and privacy roles and responsibilities; and receive approval from the system owner. 2. When contracting with external service providers: a. As part of the service contract, the AE must establish security and privacy policies and procedures for how data is stored, handled, and accessed within service provider environment; b. The data must be encrypted in transit to and from the service provider environment; c. All mechanisms used to encrypt data must be FIPS 140-2 compliant, and operate using the FIPS 140-2 compliant module; and d. Storage devices where data has resided must be securely sanitized according to MARS-E MP-6 Media Sanitization security control prior to use. e. Per SA-9 (5), the outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS.
Guidance
Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific applicable requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. **Solicitation Documents:** Solicitation documents (e.g., Request for Proposal) for any information system shall include, either explicitly or by reference, security requirements that describe the required: 1. Security capabilities; 2. Design and development processes; 3. Test and evaluation procedures; and 4. Documentation. The requirements in the solicitation documents shall permit updating security controls as new threats / vulnerabilities are identified and as new technologies are implemented. **Use of Evaluated and Validated Products:** For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet organizational requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources: 1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme; 2. The International Common Criteria Recognition Arrangements; and 3. The NIST Cryptographic Module Validation Program. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs, (b)(2)(ii), (b)(2)(iv), (b)(2)(v).

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"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the SA-4 control as described in the control requirements and associated implementation standard.

Assessment Methods and Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for information systems or services; information system design documentation; other relevant documents or records. Also examine if the organization requires providers of defined external information system to identify the location of information systems that receive, process, store, or transmit data.

Interview: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with responsibility for determining information system security functional, strength, and assurance requirements; business and/or system owners; system/network administrators; organizational personnel with information security responsibilities.

Test: Organizational processes for determining information system security functional, strength, and assurance requirements; organizational processes for developing acquisition contracts and statements of work; automated mechanisms supporting and/or implementing acquisitions and inclusion of security requirements in contracts.

Table 229. 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.	
Guidance	
Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.	
Related Control Requirement(s):	SA-5

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the SA-4 (1) control as described in the control requirements.

Assessment Methods and Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition

SA-4 (1): Functional Properties of Security Controls
documentation; acquisition contracts for information systems, system component, or information system services; other relevant documents or records. **Interview:** Organizational personnel with acquisition/contracting responsibilities; organizational personnel with responsibility for determining information system security functional requirements; information system developer or service provider; organizational personnel with information security responsibilities. **Test:** Organizational processes for determining information system security functional requirements; organizational processes for developing acquisition contracts and statements of work; automated mechanisms supporting and/or implementing acquisitions and inclusion of security requirements in contracts.

Table 230. 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, which shall include security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.	
Guidance	
Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system.	
Related Control Requirement(s):	SA-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-4 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information system, system components, or information system services; design and implementation information for security controls employed in the information system, system component, or information system service; other relevant documents or records. **Interview:** Organizational personnel with acquisition/contracting responsibilities; organizational personnel with responsibility for determining information system security requirements; information system developer or service provider; organizational personnel with information security responsibilities.	

SA-4 (2): Design/Implementation Information for Security Controls
Test: Organizational processes for determining level of detail for system design and security controls; organizational processes for developing acquisition contracts and statements of work; automated mechanisms supporting and/or implementing development of system design details.

Table 231. 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.	
Guidance	
The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources.	
Related Control Requirement(s):	CM-7, SA-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-4 (9) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; information system design documentation; information system documentation including functions, ports, protocols, and services intended for organizational use; acquisition contracts for information systems or services; acquisition documentation, solicitation documentation; service-level agreements; organizational security requirements, descriptions, and criteria for developers of information systems, system components, and information system services; other relevant documents or records. **Interview**: Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel with responsibility for determining information system security requirements; system/network administrators; organizational personnel operating, using, and/or maintaining the information system; information system developers; organizational personnel with information security responsibilities.	

Table 232. 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 documentation when such documentation is either unavailable or nonexistent. **Implementation Standards** 1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users. 2. Maintain an updated list of related system operations and security documentation. 3. Update documentation upon changes in system functions and processes. 4. Must include date and version number on all formal system documentation.	
Guidance	
This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls.	
Related Control Requirement(s):	CM-6, CM-8, PL-4, PS-2, SA-3, SA-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-5 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent information system documentation; list of actions to be taken in response to documented attempts s to obtain information system, system component, or information system service documentation; risk management strategy documentation; other relevant documents or records. **Interview:** Organizational personnel with acquisition/contracting responsibilities; organizational personnel with responsibility for determining information system security requirements; system administrators; organizational	

SA-5: Information System Documentation
personnel operating, using, and/or maintaining the information system; information system developers; organizational personnel with information security responsibilities. **Test:** Organizational processes for obtaining, protecting, and distributing information system administrator and user documentation; automated mechanisms for maintaining and monitoring system documentation including security documentations.

Table 233. SA-8: Security Engineering

SA-8: Security Engineering	
Control	
The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	
Guidance	
The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example, (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained to build secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs, (b)(2).	
Related Control Requirement(s):	PM-7, SA-3, SA-4, SC-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-8 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing security engineering principles used in the specification, design, development, and implementation, and modification of the information system; information system design documentation; information security requirements and specifications for the information system; other relevant documents or records. **Interview:** Organizational personnel with acquisition/contracting responsibilities; organizational personnel with responsibility for determining information system security requirements; organizational personnel with information system specification, design, development, implementation, and modification responsibilities; information system developers; organizational personnel with information security responsibilities. **Test:** Organizational processes for applying security engineering principles in information system specification, design, development, implementation, and modification; automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification.	

Table 234. SA-9: External Information System Services

SA-9: External Information System Services
Control The organization: a. Must notify CMS of plans to outsource information system services prior to the awarding of contract. Per SA-9 (5), the outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS. b. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; c. Defines and documents oversight and user roles and responsibilities with regard to external information system services; d. Ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance; and e. Employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security and privacy control compliance by external service providers on an ongoing basis. **Implementation Standards** 1. The service contract or agreement must include language requiring the provider to be subject to U.S. Federal laws and regulations protecting PII. 2. The service contract or agreement must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR 155.260(b), define security and privacy roles and responsibilities. 3. The AE must notify CMS at least 45 days prior to transmitting data into an external information service environment.
Guidance External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems (i.e., a service that is used by, but not a part of, the organization information system); licensing agreements; and/or supply chain exchanges. Relationships with external service providers are established in a variety of ways including, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, and lines of business arrangements), licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship delivers adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls. The external information system services documentation includes government, service providers, end user security roles and responsibilities, and service level agreements. Service level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. 5 U.S.C 552a(m) Government Contractors.— When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

SA-9: External Information System Services	
Related Control Requirement(s):	CA-3, IR-7, PS-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-9 control as described in the control requirements and associated implementation standard.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing external information system services; procedures addressing methods and techniques for monitoring security control compliance by external service providers of information system services; acquisition contracts, service-level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records. **Interview:** Organizational personnel with system and services acquisition responsibilities; external providers of information system services; organizational personnel with information security responsibilities. **Test:** Organizational processes for monitoring security control compliance by external service providers on an ongoing basis; automated mechanisms for monitoring security control compliance by external service providers on an ongoing basis.	

Table 235. SA-9 (1): Risk Assessments/Organizational Approvals

SA-9 (1): Risk Assessments/Organizational Approvals	
Control	
The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of information services. **Implementation Standards** 1. The organization documents all existing outsourced information services and conducts a risk assessment of future outsourced information services.	
Guidance	
This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraphs, (b)(2).	
Related Control Requirement(s):	CA-6, RA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-9 (1) control as described in the control requirements and associated implementation standard`.	
Assessment Methods and Objects	

SA-9 (1): Risk Assessments/Organizational Approvals
Examine: System and services acquisition policy; procedures addressing external information system services; acquisition documentation; acquisition contracts for the information system, system component, or information system service; risk assessment reports; approval records for acquisition or outsourcing of information services; other relevant documents or records. **Interview:** Organizational personnel with information system and services acquisition responsibilities; organizational personnel with information system security responsibilities; external providers of information system services. **Test:** Organizational processes for conducting a risk assessment prior to acquiring or outsourcing information services; organizational processes for approving the outsourcing of information services.

Table 236. SA-9 (2): Identification of Functions/Ports/Protocols/Services

SA-9 (2): Identification of Functions/Ports/Protocols/Services	
Control	
The organization requires providers of defined external information system services (defined in the applicable security plan) to identify the functions, ports, protocols, and other services required for the use of such services.	
Guidance	
Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.	
Related Control Requirement(s):	CM-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-9 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing external information system services; acquisition contracts for the information system, system component, or information system service; acquisition documentation; solicitation documentation; service level agreements; organizational security requirements and security specifications for external service providers; list of required functions, ports, protocols, and other services; other relevant documents or records. **Interview:** Organizational personnel with system and services acquisition responsibilities; organizational personnel with information system security responsibilities; system/network administrators; external providers of information system services.	

Table 237. SA-9 (5): Processing, Storage, and Service Location

SA-9 (5): Processing, Storage, and Service Location
Control
The outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS. Depending on the outcome of the risk assessment, the organization may need to restrict the location of

SA-9 (5): Processing, Storage, and Service Location	
information systems that receive, process, store, or transmit PII to areas within United States territories, embassies, or military installations.	
Guidance	
The location of information processing, information/data storage, or information system services that are critical to organizations, can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. External providers may use criteria for the selection of processing, storage, or service locations that are different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses and after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-9 (5) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing external information system services; acquisition contracts for the information system, system component, or information system service; solicitation documentation; acquisition documentation; service level agreements; restricted locations for information processing; information/data and/or information system services; information processing, information/data and/or information system services to be maintained in restricted locations; organizational security requirements or conditions for external providers; other relevant documents or records. **Interview:** Organizational personnel with information system security, acquisition, and contracting responsibilities; external providers of the information system services. **Test:** Organizational processes for defining requirements to restrict locations of information processing, information/data, or information services; organizational processes for ensuring the location is restricted in accordance with requirements or conditions.	

Table 238. SA-10: Developer Configuration Management

SA-10: Developer Configuration Management
Control
The organization requires the information system developers/integrators to: a. Perform configuration management during system, component, or service development, implementation, and operation; b. Document, manage, and control the integrity of changes to the information system; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles.
Guidance

SA-10: Developer Configuration Management	
The organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle.	
Related Control Requirement(s):	CM-3, CM-4, CM-9, SI-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-10 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing information system developer/integrator configuration management; solicitation documentation; acquisition documentation; acquisition contracts for the information system, system component, or information system service; service level agreements; information system developer/integrator configuration management plan; security flaw and flaw resolution tracking records; system change authorization records; change control records; configuration management records; other relevant documents or records. **Interview:** Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel with configuration management responsibilities; system developers **Test**: Organizational processes for monitoring developer configuration management; automated mechanisms supporting and/or implementing the monitoring of developer configuration management.	

Table 239. 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 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. **Implementation Standards**

SA-11: Developer Security Testing and Evaluation
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.
Guidance
Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, and binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.
Related Control Requirement(s): CA-2, CM-4, SA-3, SA-4, SA-5, SI-2
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the SA-11 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing information system developer/integrator security testing; procedures addressing flaw remediation; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the information system, system component, or information system service; system developer/integrator security test plans; records of developer security testing results for the information system, system component, or information system service; security flaw tracking records; other relevant documents or records. **Interview:** Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; system developers **Test:** Organizational processes for monitoring developer security testing and evaluation; automated mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation.

Table 240. SA-11 (1): Static Code Analysis

SA-11 (1): Static Code Analysis	
Control	
The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis. **Implementation Standards** 1. The organization submits a code analysis report as part of the authorization package and update the report in any reauthorization actions. 2. The organization documents in the Continuous Monitoring Plan how newly developed code for the information system is reviewed.	
Guidance	
Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-11 (1) control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing information system developer/integrator security testing; procedures addressing flaw remediation; solicitation documentation; acquisition documentation; service-level agreements; acquisition contracts for the information system, system component, or information system service; security flaw and remediation tracking records; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; continuous monitoring plan; other relevant documents or records. **Interview:** Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; organizational personnel with configuration management responsibilities; system developers. **Test:** Organizational processes for monitoring developer security testing and evaluation; automated mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation; static code analysis tools.	

Table 241. SA-22: Unsupported System Components

SA-22: Unsupported System Components
Control
The organization:

SA-22: Unsupported System Components	
a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	
Guidance	
Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.	
Related Control Requirement(s):	PL-2, SA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SA-22 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and services acquisition policy; procedures addressing replacement or continued use of unsupported information system components; documented evidence of replacing unsupported information system components; documented approvals (including justification) for continued use of unsupported information system components; information system inventory records; security assessment results. **Interview:** Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for system development life cycle; organizational personnel responsible for configuration management; organizational personnel responsibility for information system components. **Test:** Organizational processes for replacing unsupported system components; automated mechanisms supporting and/or implementing replacement of unsupported system components.	

1.29 System and Communications Protection (SC)

Table 242. SC-1: System and Communications Protection Policy and Procedures

SC-1: System and Communications Protection Policy and Procedures	
Control	
The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the System and Communication Protection (SC) family. Policy and procedures reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing SC policy and procedures.	
Related Control Requirement(s):	PM-9
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy and procedures; and other relevant documents or records. **Interview:** Organizational personnel with system and communications protection responsibilities; organizational personnel with information security responsibilities.	

Table 243. SC-2: Application Partitioning

SC-2: Application Partitioning
Control
The information system separates user functionality, including user interface services (e.g., web services), from information system management (e.g., database management systems) functionality.
Guidance
Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of

SC-2: Application Partitioning	
user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.	
Related Control Requirement(s):	SA-4, SA-8
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-2 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer. **Test:** Separation of user functionality from information system management functionality.	

Table 244. 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.
Guidance
This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, and hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address (i) information remanence, which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles.

SC-4: Information in Shared Resources	
Related Control Requirement(s):	AC-3, AC-4, MP-6

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the SC-4 control as described in the control requirements and associated implementation standards.

Assessment Methods and Objects

Examine: System and communications protection policy; procedures addressing information protection in shared system resources; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities; system developer.

Test: Automated mechanisms preventing unauthorized and unintended transfer of information via shared system resources.

Table 245. 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 on the following websites by employing security safeguards (defined in the applicable security plan): a. SANS Organization: www.sans.org/dosstep ; b. SANS Organization's Roadmap to Defeating DDoS: www.sans.org/dosstep ; and c. 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.	
Guidance	
A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.	
Related Control Requirement(s):	SC-6, SC-7

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the SC-5 control as described in the control requirements and associated implementation standards.

SC-5: Denial of Service Protection
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; list of denial of services attacks requiring employment of security safeguards to protect against or limit effects of such attacks; list of security safeguards protecting against or limiting the effects of denial of service attacks; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer. **Test:** Automated mechanisms protecting against or limiting the effects of denial of service attacks.

Table 246. 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.	
Guidance	
Priority protection helps prevent lower-priority processes from delaying or interfering with the information system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to information system components for which there are only single users/roles.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-6 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing prioritization of information system resources; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer. **Test:** Automated mechanisms supporting and/or implementing resource allocation capability; safeguards employed to protect availability of resources.	

Table 247. SC-7: Boundary Protection

SC-7: Boundary Protection
Control
The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

SC-7: Boundary Protection	
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 at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.	
Guidance	
Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-7 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; network architecture diagram; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities. **Test:** Automated mechanisms implementing boundary protection capability.	

Table 248. SC-7 (3): Access Points

SC-7 (3): Access Points	
Control	
The organization limits the number of external network connections to the information system.	
Guidance	
Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-7 (3) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; communications and network traffic monitoring logs; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities. **Test:** Automated mechanisms implementing boundary protection capability; automated mechanisms limiting the number of external network connections to the information system.	

Table 249. 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. Employs security controls as needed to protect the confidentiality and integrity of the information transmitted; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; e. Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days; and f. Removes traffic flow policy 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"	
Assessment Procedure:	

SC-7 (4): External Telecommunications Services
Assessment Objective Determine if the organization has implemented all elements of the SC-7 (4) control as described in the control requirements.
Assessment Methods and Objects **Examine:** System and communications protection policy; traffic flow policy; information flow control policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; records of traffic flow policy exceptions; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities. **Test:** Organizational processes for documenting and reviewing exceptions to the traffic flow policy; organizational processes for removing exceptions to the traffic flow policy; automated mechanisms implementing boundary protection capability; managed interfaces implementing traffic flow policy.

Table 250. 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).	
Guidance	
This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections that are essential and approved are allowed.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-7 (5) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; network device hardware/software configuration; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities. **Test:** Automated mechanisms implementing traffic management at managed interfaces.	

Table 251. SC-7 (7): Prevent Split Tunneling for Remote Devices

SC-7 (7): Prevent Split Tunneling for Remove Drivers	
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.	
Guidance	
This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers; however, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of Virtual Private Networks (VPN) for remote connections that are adequately provisioned with appropriate security controls may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-7 (7) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities. **Test:** Automated mechanisms implementing boundary protection capability; automated mechanisms supporting/restricting non-remote connections.	

Table 252. SC-7 (8): Route Traffic to Authenticated Proxy Servers

SC-7 (8): Route Traffic to Authenticated Proxy Servers
Control
The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices. **Implementation Standards**

SC-7 (8): Route Traffic to Authenticated Proxy Servers	
1. 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.	
Guidance	
External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URL), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.	
Related Control Requirement(s):	AC-3, AU-2
Control Implementation Description:	
"Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-7 (8) control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities. **Test:** Automated mechanisms implementing boundary protection capability; automated mechanisms supporting/restricting non-remote connections.	

Table 253. 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.	
Guidance	
Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.	
Related Control Requirement(s):	
Control Implementation Description:	
"Click here and type text"	

SC-7 (12): Host-Based Protection
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the SC-7 (12) control as described in the control requirements.
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; information system audit records; "host-based" boundary protection hardware and software; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities; information system users. **Test:** Automated mechanisms implementing host-based boundary protection capability.

Table 254. 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.	
Guidance	
Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations.	
Related Control Requirement(s):	SA-8, SC-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-7 (13) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; list of security tools and support components to be isolated from other internal information system components; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities. **Test:** Automated mechanisms supporting and/or implementing isolation of information security tools, mechanisms, and support components.	

Table 255. 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.	
Guidance	
Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to the devices, or cause information external to the devices, to enter the devices, nor can failures permit unauthorized information releases.	
Related Control Requirement(s):	CP-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-7 (18) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system architecture; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities. **Test:** Automated mechanisms supporting and/or implementing secure failure.	

Table 256. SC-8: Transmission Confidentiality and Integrity

SC-8: Transmission Confidentiality and Integrity
Control
The information system protects the confidentiality and integrity of transmitted information. **Implementation Standards** 1. Employ appropriate approved mechanisms (e.g., digital signatures and cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13).
Guidance
This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services that can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality / integrity services are available in standard,

SC-8: Transmission Confidentiality and Integrity	
commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(vi)	
Related Control Requirement(s):	AC-17, PE-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-8 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing transmission confidentiality and integrity; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer. **Test:** Automated mechanisms supporting and/or implementing transmission confidentiality and/or integrity.	

Table 257. 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 defined alternative physical safeguards (defined in the applicable security plan). This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(6).	
Guidance	
Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions that have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.	
Related Control Requirement(s):	SC-13
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-8 (1) control as described in the control requirements.	

SC-8 (1): Cryptographic or Alternate Physical Protection
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer. **Test:** Cryptographic mechanisms supporting and/or implementing transmission confidentiality and/or integrity; automated mechanisms supporting and/or implementing alternative physical safeguards; organizational processes for defining and implementing alternative physical safeguards.

Table 258. 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.	
Guidance	
Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.	
Related Control Requirement(s):	AU-10
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-8 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer. **Test:** Automated mechanisms supporting and/or implementing transmission confidentiality and/or integrity.	

Table 259. SC-10: Network Disconnect

SC-10: Network Disconnect
Control
The information system terminates the network connection associated with a communications session at the end of the session, or:

SC-10: Network Disconnect
a. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and b. Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes or less of inactivity.
Guidance
This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses. A session is an encounter between an end-user interface device (e.g., computer, terminal, or process) and an application, including a network logon—the AC-11 session lock applies. A connection-based session is one that requires a connection to be established between hosts prior to an exchange of data.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the SC-10 control as described in the control requirements.
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer. **Test:** Automated mechanisms supporting and/or implementing network disconnect capability.

Table 260. 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.
Guidance
Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.

SC-12: Cryptographic Key Establishment and Management	
Related Control Requirement(s):	SC-13, SC-17
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-12 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing cryptographic key management and establishment; information system design documentation; cryptographic mechanisms; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for cryptographic key establishment and/or management. **Test:** Automated mechanisms supporting and/or implementing cryptographic key establishment and management.	

Table 261. SC-12 (2): Symmetric Keys

SC-12 (2): Symmetric Keys	
Control	
The organization produces, controls, and distributes symmetric cryptographic keys using organization-defined key management technology and processes.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-12 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of FIPS-validated cryptographic products; list of National Security Agency-approved cryptographic products; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic key establishment or management. **Test:** Automated mechanisms supporting and/or implementing symmetric cryptographic key establishment and management.	

Table 262. SC-13: Cryptographic Protection

SC-13: Cryptographic Protection	
Control	
When cryptographic mechanisms are used, the information system implements encryption products that have been validated under the Cryptographic Module Validation Program (see http://csrc.nist.gov/groups/STM/cmvp/validation.html) to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, directives, policies, regulations, and standards.	
Guidance	
Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography; however, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-13 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic protection. **Test:** Automated mechanisms supporting and/or implementing cryptographic protection.	

Table 263. SC-15: Collaborative Computing Device

SC-15: Collaborative Computing Device
Control
The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the organization's CIO or designated representative. If collaborative computing is authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system used on the collaborative computing mechanisms. The information system: a. Prohibits remote activation of collaborative computing devices; and b. Provides an explicit indication of use to users physically present at the devices.
Guidance

SC-15: Collaborative Computing Device	
Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.	
Related Control Requirement(s):	AC-21
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-15 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing collaborative computing devices. **Test**: Automated mechanisms supporting and/or implementing management of remote activation of collaborative computing devices; automated mechanisms providing an indication of use of collaborative computing devices.	

Table 264. 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.	
Guidance	
For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services.	
Related Control Requirement(s):	SC-12
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-17 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; other relevant documents or records.	

SC-17: Public Key Infrastructure Certificates
Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with public key infrastructure certificate issuing responsibilities; service providers. **Test:** Automated mechanisms supporting and/or implementing the management of public key infrastructure certificates.

Table 265. 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.	
Guidance	
Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smartphones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.	
Related Control Requirement(s):	AU-2, AU-12, CM-2, CM-6, SI-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-18 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; authorization records; information system monitoring records; information system audit records; information system configuration settings; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with mobile code authorization, monitoring, and control responsibilities. **Test:** Organizational process for controlling, authorizing, monitoring, and restricting mobile code; automated mechanisms supporting and/or implementing the management of mobile code; automated mechanisms supporting and/or implementing the monitoring of mobile code.	

Table 266. SC-19: Voice Over Internet Protocol

SC-19: Voice Over Internet Protocol	
Control	
The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CIO or designated representative. If authorized, the organization: a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	
Related Control Requirement(s):	CM-6, SC-7, SC-15
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-19 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; VoIP implementation guidance; information system design documentation; information system configuration settings and associated documentation; information system monitoring records; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing VoIP. **Test:** Organizational process for authorizing, monitoring, and controlling VoIP; automated mechanisms supporting and/or implementing authorizing, monitoring, and controlling VoIP.	

Table 267. SC-20: Secure Name/Address Resolution Service

SC-20: Secure Name/Address Resolution Service
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. **Implementation Standards** 1. Recursive lookups are disabled on all publicly accessible domain name system (DNS) servers.
Guidance
This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information

SC-20: Secure Name/Address Resolution Service	
systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.	
Related Control Requirement(s):	AU-10, SC-8, SC-12, SC-13, SC-21, SC-22
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-20 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS. **Test:** Automated mechanisms supporting and/or implementing secure name/address resolution service.	

Table 268. SC-21: Secure Name/Address Resolution Service

SC-21: Secure Name/Address Resolution Service	
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.	
Guidance	
Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNS Security (DNSSEC) signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.	
Related Control Requirement(s):	SC-22
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-21 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system	

SC-21: Secure Name/Address Resolution Service
configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview**: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS. **Test:** Automated mechanisms supporting and/or implementing data origin authentication and data integrity verification for name/address resolution services].

Table 269. 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.	
Guidance	
Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges and explicit lists).	
Related Control Requirement(s):	SC-2, SC-21
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-22 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS. **Test:** Automated mechanisms supporting and/or implementing name/address resolution service for fault tolerance and role separation.	

Table 270. SC-23: Session Authenticity

SC-23: Session Authenticity	
Control	
The information system protects the authenticity of communications sessions.	
Guidance	
This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.	
Related Control Requirement(s):	SC-8, SC-10
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-23 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities. **Test:** Automated mechanisms supporting and/or implementing session authenticity.	

Table 271. 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. **Implementation Standards** Sensitive information such as PII should be encrypted while at rest. If information in the service provider environment cannot be encrypted, appropriate data isolation is a potential compensating control. All mechanisms used to encrypt data must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module. This requirement must be included in the SLA, if applicable.
Guidance
This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.

SC-28: Protection of Information at Rest	
This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(3)(vi).	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-28 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developer. **Test:** Automated mechanisms supporting and/or implementing confidentiality and integrity protections for information at rest.	

Table 272. SC-32: Information System Partitioning

SC-32: Information System Partitioning	
Control	
The organization partitions the information system into defined information system components (defined in the applicable security plan) residing in separate physical domains or environments based on defined circumstances (defined in the applicable security plan) for physical separation of components. **Implementation Standards** When contracting with external service providers, Personally Identifiable Information (PII), as well as software and services that receive, process, store, or transmit PII must be isolated within the service provider environment to the maximum extent possible so that other service provider customers sharing physical or virtual space cannot gain access to such data or applications.	
Guidance	
Information system partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.	
Related Control Requirement(s):	AC-4, SA-8, SC-2, SC-7
Control Implementation Description: "Click here and type text"	

SC-32: Information System Partitioning
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the SC-32 control as described in the control requirements.
Assessment Methods and Objects **Examine:** System and communications protection policy; procedures addressing information system partitioning; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of information system physical domains (or environments); information system facility diagrams; information system network diagrams; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; information system developers/integrators. **Test:** Automated mechanisms supporting and/or implementing physical separation of information system components.

Table 273. SC-39: Process Isolation

SC-39: Process Isolation	
Control	
The information system maintains a separate execution domain for each executing process.	
Guidance	
Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space, which permits the security functions to control the manner of communication between processes, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.	
Related Control Requirement(s):	AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-39 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information system design documentation; information system configuration settings and associated documentation; information system architecture; independent verification and validation documentation; testing and evaluation documentation, other relevant documents or records. **Interview:** Information system developers/integrators; information system security architect. **Test:** Automated mechanisms supporting and/or implementing separate execution domains for each executing process.	

Table 274. SC-ACA-1: Electronic Mail

SC-ACA-1: Electronic Mail
Control
Controls shall be implemented to protect sensitive information that is sent via email. **Implementation Standards** 1. Prior to sending an email, place all sensitive information in an encrypted attachment.
Guidance
Recommended security practices for handling sensitive information via e-mail can be found in NIST SP 800-45 (as amended), *Guidelines on Electronic Mail Security*.
Related Control Requirement(s):
Control Implementation Description: "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the SC-ACA-1 control as described in the control requirements and associated implementation standards.
Assessment Methods and Objects **Examine:** Email policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with responsibility for security and a sample of organizational personnel who use email.

Table 275. SC-ACA-2: FAX Usage

SC-ACA-2: FAX Usage
Control
If Personally Identifiable Information (PII) is allowed to be included with fax communications, the organization establishes policies and procedures for handling fax transmissions. The organization must follow specific precautions and Implementation Standards when performing fax transmission of PII: a. Transmit PII only to an authorized recipient **Implementation Standards** 1. When sending or receiving faxes containing PII: a. Fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; b. Accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and c. A cover sheet must be used that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.
Guidance

SC-ACA-2: FAX Usage	
Do not send PII over FAX unless it *cannot* be sent over other, more secure, channels, i.e., delivery by hand, secure email, etc.	
Related Control Requirement(s):	PE-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SC-ACA-2 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Fax handling policy and procedures addressing the protection of PII. **Examine:** Fax machine locations for secure custodial coverage of outgoing and incoming PII transmitted data. **Interview:** Organizational personnel with responsibility for security and organizational personnel with responsibility for handling fax transmissions.	

1.30 System and Information Integrity (SI)

Table 276. SI-1: System and Information Integrity Policy and Procedures

SI-1: System and Information Integrity Policy and Procedures	
Control	
The organization develops, disseminates, and distributes to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	
Guidance	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the System and Information Integrity (SI) family. Policy and procedures reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the Administering Entity (AE) organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-1 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy and procedures; and other relevant documents or records. **Interview:** Organizational personnel with system and information integrity responsibilities; organizational personnel with information security responsibilities.	

Table 277. 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 on production equipment within a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw as follows:

SI-2: Flaw Remediation
flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days; and d. Incorporates flaw remediation into the organizational configuration management process with risk-based decisions if a security patch is not applied to a security-based system or network authorized by the organization.
Guidance
Organizations identify information systems affected by announced software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, and hot fixes. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, organizations can track and verify required / anticipated remediation actions. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow the United States Computer Emergency Response Team (US-CERT) guidance and Information Assurance Vulnerability Alerts. Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical. The System Owner may also consider in testing decisions whether security-relevant software or firmware updates are obtained from authorized sources.
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"
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the SI-2 control as described in the control requirements.
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; installation/change control records for security-relevant software and firmware updates; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with flaw remediation responsibilities; organizational personnel with configuration management responsibility. **Test:** Organizational processes for identifying, reporting, and correcting information system flaws; organizational process for installing software and firmware updates; automated mechanisms supporting and/or implementing reporting, and correcting information system flaws; automated mechanisms supporting and/or implementing testing software and firmware updates.

Table 278. SI-2 (1): Central Management

SI-2 (1): Central Management Enhancement	
Control	
The organization centrally manages the flaw remediation process.	
Guidance	
Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined flaw remediation security controls.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-2 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records. **Interview**: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for flaw remediation. **Test:** Organizational processes for central management of the flaw remediation process; automated mechanisms supporting and/or implementing central management of the flaw remediation process.	

Table 279. SI-2 (2): Automated Flaw Remediation Status

SI-2 (2): Automated Flaw Remediation Status	
Control	
The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-2 (2) control as described in the control requirements.	
Assessment Methods and Objects	

SI-2 (2): Automated Flaw Remediation Status
Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for flaw remediation. **Test:** Automated mechanisms used to determine the state of information system components with regard to flaw remediation.

Table 280. 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 Administering Entity (AE) configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform desktop and critical system file scans every twenty-four (24) hours, 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 AE organizational security policy; 2. Block and quarantine malicious code and send alerts to the 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.
Guidance
Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE or Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards, including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.

SI-3: Malicious Code Protection	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-3 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system design documentation; information system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with malicious code protection responsibilities; organizational personnel with configuration management responsibility. **Test:** Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; automated mechanisms supporting and/or implementing employing, updating, and configuring malicious code protection mechanisms; automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions.	

Table 281. SI-3 (1): Central Management

SI-3 (1): Central Management	
Control	
The organization centrally manages malicious code protection mechanisms.	
Guidance	
Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined security controls for flaw and malicious code protection.	
Related Control Requirement(s):	AU-2, SI-8
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-3 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing malicious code protection; automated mechanisms supporting centralized management of malicious code protection mechanisms; information system	

SI-3 (1): Central Management
design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for malicious code protection. **Test:** Organizational processes for central management of malicious code protection mechanisms; automated mechanisms supporting and/or implementing central management of malicious code protection mechanisms.

Table 282. SI-3 (2): Automatic Updates

SI-3 (2): Automatic Updates	
Control	
The information system automatically updates malicious code protection mechanisms.	
Guidance	
Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations carefully consider the methodology to carry out automatic updates.	
Related Control Requirement(s):	SI-8
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-3 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing malicious code protection; automated mechanisms supporting centralized management of malicious code protection mechanisms; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for malicious code protection. **Test:** Automated mechanisms supporting and/or implementing automatic updates to malicious code protection capability.	

Table 283. SI-4: Information System Monitoring

SI-4: Information System Monitoring
Control
The organization: a. Monitors the information system to detect:

SI-4: Information System Monitoring
1. Attacks and indicators of potential attacks in accordance with the current Administering Entity (AE) organization incident handling policy and procedure; and 2. Unauthorized local, network, and remote connections; b. Monitors events on the information system to ensure the proper functioning of internal processes and controls; c. Examines system records to confirm that the system is functioning in an optimal, resilient, and secure state; d. Identifies irregularities or anomalies that are indicators of a system malfunction or compromise, and detects information system attacks; e. Monitors for unauthorized remote connections to the information system continuously in real time, and takes appropriate action if an unauthorized connection is discovered; f. Identifies unauthorized use of the information system through defined techniques and methods (defined in the applicable security plan); g. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; h. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; i. 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; j. Obtains legal opinion with regard to information system-monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations; and k. Provides specified information system monitoring information to defined personnel or roles as needed, and at the established frequency (all as defined in the applicable security plan). **Implementation Standards** 1. Install Intrusion Detection"/Prevention" System (IDS"/IPS") devices at network perimeter points and host-based IDS"/IPS" sensors on critical servers.
Guidance
Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications. Typically, these devices are employed at the managed interfaces associated with controls SC-7 and AC-17. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

SI-4: Information System Monitoring	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-4 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Continuous monitoring strategy; system and information integrity policy; procedures addressing information system monitoring tools and techniques; facility diagram/layout; information system design documentation; information system monitoring tools and techniques documentation; locations within information system where monitoring devices are deployed; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility monitoring the information system. **Test:** Organizational processes for information system monitoring; automated mechanisms supporting and/or implementing information system monitoring capability.	

Table 284. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-4 (1) control as described in the control requirements [and associated implementation standards].	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for the intrusion detection system.	

SI-4 (1): System-Wide Intrusion Detection System
Test: Organizational processes for intrusion detection/information system monitoring; automated mechanisms supporting and/or implementing intrusion detection capability.

Table 285. SI-4 (2): Automated Tools for Real-Time Analysis

SI-4 (2): Automated Tools for Real-Time Analysis	
Control	
The organization employs automated tools to support near real-time analysis of events.	
Guidance	
Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real-time analysis of alerts and/or notifications generated by organizational information systems.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-4 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools; monitoring techniques documentation; information system configuration settings and associated documentation; information system audit records; information system protocols documentation; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for incident response/management. **Test:** Organizational processes for near real-time analysis of events; organizational processes for information system monitoring; automated mechanisms supporting and/or implementing information system monitoring; automated mechanisms/tools supporting and/or implementing analysis of events.	

Table 286. 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 security plan) for unusual or unauthorized activities or conditions.
Guidance
Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, (i) internal traffic that indicates the presence of malicious code within organizational information systems or (ii) propagating among system components the unauthorized exporting of information or

SI-4 (4): Inbound and Outbound Communications Traffic	
signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-4 (4) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for the intrusion detection system. **Test:** Organizational processes for intrusion detection/information system monitoring; automated mechanisms supporting and/or implementing intrusion detection capability/information system monitoring; automated mechanisms supporting and/or implementing monitoring of inbound/outbound communications traffic.	

Table 287. 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 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.
Guidance
Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/Business Owners, System Owners, or information system security officers. The indications that a compromise or potential compromise occurred include modification of protected information system files or directories without notification from the appropriate change/configuration management channels; information system performance indicating resource consumption that is inconsistent with expected operating conditions; auditing functionality that has been disabled or modified to reduce audit visibility; audit or log records that have been deleted or modified without explanation; the 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; the information system reports failed logins or

SI-4 (5): System-Generated Alerts	
password changes for administrative or key service accounts; processes and services are running that are outside of the baseline system profile; and 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
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-4 (5) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; alerts/notifications generated based on compromise indicators; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for the intrusion detection system. **Test:** Organizational processes for intrusion detection/information system monitoring; automated mechanisms supporting and/or implementing intrusion detection/information system monitoring capability; automated mechanisms supporting and/or implementing alerts for compromise indicators.	

Table 288. SI-4 (14): Wireless Intrusion Detection

SI-4 (14): Wireless Intrusion Detection	
Control	
The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	
Guidance	
Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing information systems, but also include areas outside of facilities, as needed, to verify that unauthorized wireless access points are not connected to the systems. A Wireless Intrusion Detection/Wireless Intrusion Detection (WIDS/WIPS) system is recommended.	
Related Control Requirement(s):	AC-18, IA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-4 (14) control as described in the control requirements.	

SI-4 (14): Wireless Intrusion Detection
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; information system audit records; other relevant documents or records. **Interview:** System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibilities associated with intrusion detection systems. **Test:** Organizational processes for intrusion detection; automated mechanisms supporting and/or implementing wireless intrusion detection capability.

Table 289. 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 (defined in the applicable security plan) on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: defined personnel or roles with system administration, monitoring, and/or security responsibilities (defined in the applicable security plan); and d. Implements security directives in accordance with established timeframes, or notifies the business owner of the degree of noncompliance.	
Guidance	
The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness. Compliance with security alerts and directives is essential because of their critical nature and the potential immediate adverse effects on organizational operations and assets, individuals, or other external organizations. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.	
Related Control Requirement(s):	SI-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-5 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing security alerts, advisories, and directives; records of security alerts and advisories; other relevant documents or records. **Interview:** Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system; organizational personnel, organizational elements, and/or external organizations to whom alerts, advisories, and directives are to be disseminated; system/network administrators; organizational personnel with information security responsibilities.	

SI-5: Security Alerts, Advisories, and Directives
Test: Organizational processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives; automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives; automated mechanisms supporting and/or implementing security directives.

Table 290. SI-6: Security Function Verification

SI-6: Security Function Verification	
Control	
The information system: a. Verifies the correct operation of defined security functions (defined in the applicable security plan); b. Performs this verification upon system startup and restart; upon command by the administrator with appropriate privilege, periodically on a monthly basis; c. Notifies system administration of failed security verification tests; and d. Shuts the information system down, restarts the information system, or performs some other defined alternative action(s) (defined in the applicable security plan) when anomalies are discovered.	
Guidance	
Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights.	
Related Control Requirement(s):	CA-7, CM-6
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-6 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; alerts/notifications of failed security verification tests; list of system transition states requiring security functionality verification; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with security function verification responsibilities; organizational personnel implementing, operating, and maintaining the information system; system/network administrators; organizational personnel with information security responsibilities; system developer. **Test:** Security function verification capability and automated mechanisms supporting and/or implementing security function verification capability.	

Table 291. 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.	
Guidance	
Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, and cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.	
Related Control Requirement(s):	SC-8, SC-13, SI-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-7 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records generated/triggered from integrity verification tools regarding unauthorized software, firmware, and information changes; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibility for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators. **Test:** Software, firmware, and information integrity verification tools.	

Table 292. SI-7 (1): Integrity Checks

SI-7 (1): Integrity Checks	
Control	
The organization reassesses the integrity of software and information by performing daily integrity scans of the information system.	
Guidance	
Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	

SI-7 (1): Integrity Checks
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the SI-7 (1) control as described in the control requirements.
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing software and information integrity; information system design documentation; security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records. **Interview:** Organizational personnel with responsibility for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer. **Test:** Software, firmware, and information integrity verification tools.

Table 293. SI-7 (7): Integration of Detection and Response

SI-7 (7): Integration of Detection and Response	
Control	
The organization incorporates the detection of unauthorized security-relevant changes to the organizational incident response capability of the information system (defined in the applicable security plan).	
Guidance	
This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for identifying and discerning adversary actions over an extended period and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.	
Related Control Requirement(s):	IR-4, IR-5, SI-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-7 (7) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing software firmware, and information integrity; procedures addressing incident response; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; incident response records; information audit records; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records. **Interview:** Organizational personnel with responsibility for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities. **Test:** Organizational processes for incorporating detection of unauthorized security-relevant changes into the incident response capability; software, firmware, and information integrity verification tools; automated	

SI-7 (7): Integration of Detection and Response
mechanisms supporting and/or implementing incorporation of detection of unauthorized security-relevant changes into the incident response capability.

Table 294. 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.	
Guidance	
Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.	
Related Control Requirement(s):	AT-2, AT-3, SC-5, SC-7, SI-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-2 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; configuration management policy and procedures; procedures addressing spam protection; records of spam protection updates; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with spam protection responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developer. **Test:** Organizational processes for implementing spam protection; automated mechanisms supporting and/or implementing spam protection.	

Table 295. SI-8 (1): Central Management

SI-8 (1): Central Management
Control
The organization centrally manages spam protection mechanisms.
Guidance

SI-8 (1): Central Management	
Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined spam protection security controls.	
Related Control Requirement(s):	AU-3, SI-2, SI-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-8 (1) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview**: Organizational personnel with responsibility for spam protection; organizational personnel with information security responsibilities; system/network administrators. **Test:** Organizational processes for central management of spam protection; automated mechanisms supporting and/or implementing central management of spam protection.	

Table 296. 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"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-8 (2) control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; records of spam protection updates; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibility for spam protection; organizational personnel with information security responsibilities; system/network administrators; system developer. **Test:** Organizational processes for spam protection; automated mechanisms supporting and/or implementing automatic updates to spam protection mechanisms.	

Table 297. SI-10: Information Input Validation

SI-10: Information Input Validation	
Control	
The information system checks the validity of defined information inputs (defined in the applicable security plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.	
Guidance	
Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a) (3)(vi).	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-10 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing information input validation; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify validity of information; information system design documentation; information system configuration settings and associated documentation; procedures addressing information input validation; other relevant documents or records. **Interview:** Organizational personnel with responsibility for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer. **Test:** Automated mechanisms supporting and/or implementing validity checks on information inputs.	

Table 298. 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 information that could be exploited by adversaries; and b. Reveals error messages only to defined personnel or roles (defined in the applicable security plan).
Guidance

SI-11: Error Handling	
Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username; mission/business information that can be derived from (if not stated explicitly by) information recorded; 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 or access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, and object permission attributes and settings in error logs and administrative messages that could be exploited by adversaries; and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information.	
Related Control Requirement(s):	AU-2, AU-3, SI-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-11 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; documentation providing structure/content of error messages; information system audit records; other relevant documents or records. **Interview:** Organizational personnel with responsibility for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer. **Test:** Organizational processes for error handling; automated mechanisms supporting and/or implementing error handling; automated mechanisms supporting and/or implementing management of error messages	

Table 299. 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 Standards** 1. 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 Administering Entity organizational requirements, whichever is more restrictive.
Guidance
Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. NARA policy applies to the retention of federal data residing held by Administering Entities.

SI-12: Information Handling and Retention	
This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(4)(vi).	
Related Control Requirement(s):	AU-5, AU-11, MP-2, MP-4, DM-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-12 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** System and information integrity policy, directives, policies, regulations, standards, and operational requirements applicable to information handling and retention; media protection policy and procedures; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records; other relevant documents or records. **Interview:** Organizational personnel with information output handling and retention responsibilities organizational personnel with information security responsibilities/network administrators. **Test:** Organizational processes for information handling and retention; automated mechanisms supporting and/or implementing information handling and retention.	

Table 300. SI-16: Memory Protection

SI-16: Memory Protection	
Control	
The information system implements security safeguards to protect its memory from unauthorized code execution.	
Guidance	
Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware enforced or software enforced with hardware providing the greater strength of mechanism.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the SI-16 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** System integrity policy and procedures; procedures addressing memory protection for the information system; information system design documentation; information system configuration settings and associated documentation; list of security safeguards protecting information system memory from unauthorized code execution; information system audit records; products in place to protect unauthorized code execution.	

SI-16: Memory Protection
Interview: Organizational personnel with responsibilities associated with products that protect memory from unauthorized code execution; organizational personnel with information security responsibilities; system/network administrators; system developer. **Test:** Automated mechanisms supporting and/or implementing safeguards to protect information system memory from unauthorized code execution.

1.31 Program Management (PM)

Table 301. PM-1: Information Security Program Plan

PM-1: Information Security Program Plan	
Control	
The organization: a. Develops and disseminates an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, and cyber-physical); and 4. Is approved by a senior official with responsibility and accountability for the risk incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan within every three hundred sixty-five (365) days; c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the information security program plan from unauthorized disclosure and modification.	
Guidance	
Information security program plans can be represented in single documents or compilations of documents at the discretion of the System Owner. These plans document the program management controls and organization-defined common controls. They provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable (a) implementations that are unambiguously compliant with the intent of the plans and (b) a determination of the risk incurred if the plans are implemented as intended. Together, the security plans for individual information systems and the organization-wide information security program plan provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the descriptions of common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document which organizational official or officials are responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the Physical and Environmental Protection (PE) family when such controls are not associated with a particular information system but instead support multiple information systems.	
Related Control Requirement(s):	PM-8
Control Implementation Description: "Click here and type text"	

PM-1: Information Security Program Plan
Assessment Procedure:
Assessment Objective Determine if the organization has implemented all elements of the PM-1 control as described in the control requirements.
Assessment Methods and Objects **Examine:** Information security program plan and policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; procedures addressing coordination of the program plan with relevant entities; procedures for program plan approvals; records of program plan reviews and updates; common controls documentation; other relevant documents or records. **Interview:** Organizational personnel with security planning and plan implementation responsibilities for the information security program; organizational personnel with information security responsibilities. **Test:** Organizational processes for information security program plan development/review/update/approval; automated mechanisms supporting and/or implementing the information security program plan.

Table 302. PM-2: Senior Information Security Officer

PM-2: Senior Information Security Officer	
Control	
The organization appoints a senior information security officer with the responsibility and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	
Guidance	
The security officer described in this control is an organizational official. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.	
Related Control Requirement(s):	
Control Implementation Description: «Click here and type text.]»	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-2 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; procedures addressing program plan development and implementation; procedures addressing program plan reviews and updates; procedures addressing coordination of the program plan with relevant entities; documentation addressing roles and responsibilities of the senior information security officer position; information security program mission statement; other relevant documents or records. **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational person appointed to the senior information security officer position; organizational personnel with information security responsibilities.	

Table 303. PM-3: Information Security Resources

PM-3: Information Security Resources	
Control	
The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	
Guidance	
Organizations consider establishing champions for information security efforts and, as part of that action, include the necessary resources and assign the specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process.	
Related Control Requirement(s):	PM-4, SA-2
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-3 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; capital planning and investment policy; procedures addressing management and oversight for information security-related aspects of the capital planning and investment control process; capital planning and investment documentation; documentation of exceptions supporting capital planning and investment requests; business cases; other relevant documents or records. **Interview:** Organizational personnel managing and overseeing the information security-related aspects of the capital planning and investment control process; organizational personnel with information security program planning responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for capital planning and investment; organizational processes for business case development; automated mechanisms supporting the capital planning and investment process.	

Table 304. PM-4: Plan of Action and Milestones Process

PM-4: Plan of Action and Milestones Process
Control
The organization: a. Implements a process to ensure that plans of action and milestones (POA&M) for the security program and associated organizational information systems: 1. Are developed and maintained; 2. Document the remedial information security actions to adequately respond to risks to organizational operations and assets, individuals, other organizations, and the Nation; 3. Are reported in accordance with CMS reporting requirements; and b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions

PM-4: Plan of Action and Milestones Process	
Implementation Standards 1. CMS Reporting Requirement: AEs must submit copies of their updated POA&M to CMS on a quarterly basis. The POA&M template (an Excel spreadsheet) used to report the status of POA&M can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Guidance	
The plan of action and milestones is a key document in the information security program and is subject to reporting requirements established by CMS. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Updates to plans of action and milestones are based on findings from security control assessments and continuous monitoring activities. CMS provides submission requirements and due dates for the POA&M in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	CA-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-4 control as described in the control requirements and associated implementation standards.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; plan of action and milestones; procedures addressing plan of action milestones development and maintenance; procedures addressing plan of action and milestones reporting; procedures for review of plan of action and milestones for consistency with risk management strategy and risk response priorities; results of risk assessments associated with plan of action and milestones; plan of action and milestones for organizational information systems; other relevant documents or records. **Interview:** Organizational personnel with responsibility for developing, maintaining, reviewing, and reporting plans of action and milestones; organizational personnel with information security responsibilities. **Test:** Organizational processes for plan of action and milestones development, review, maintenance, reporting; automated mechanisms supporting plans of action and milestones maintenance, review and update.	

Table 305. PM-5: Information System Inventory

PM-5: Information System Inventory
Control
The organization develops and maintains an inventory of its information systems.
Guidance
This control addresses the inventory requirements as documented in system configuration management policy and procedures and in Security Control CM-8.

PM-5: Information System Inventory	
Related Control Requirement(s):	CM-1, CM-8, SE-1
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-5 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; information system inventory; procedures addressing information system inventory development and maintenance; information system inventory records; other relevant documents or records. **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel with information system inventory development and maintenance responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for information system inventory development and maintenance; automated mechanisms supporting the information system inventory.	

Table 306. PM-6: Information Security Measures of Performance

PM-6: Information Security Measures of Performance	
Control	
The organization develops, monitors, and reports on the results of information security measures of performance.	
Guidance	
Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.	
Related Control Requirement(s):	
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-6 control as described in the control requirements.	
Assessment Methods and Objects	

PM-6: Information Security Measures of Performance
Examine: Information security program plan and policy; information security measures of performance; information system inventory; procedures addressing development, monitoring, and reporting of information security performance measures; results of information security performance measures; other relevant documents or records. **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for developing, monitoring, and reporting information security measures of performance; organizational personnel with information security responsibilities. **Test:** Organizational processes for developing, monitoring, and reporting information security measures of performance; automated mechanisms supporting the development, monitoring, and reporting of information security measures of performance.

Table 307. PM-7: Enterprise Architecture

PM-7: Enterprise Architecture	
Control	
The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	
Guidance	
The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that the organization addresses security considerations early in the system development life cycle and that these security considerations are directly and explicitly related to the organization's mission/business processes. Through this process of security requirements integration, the organization embeds into the enterprise architecture an integral information security architecture consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system, but at the same time is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the risk management framework and supporting security standards and guidelines.	
Related Control Requirement(s):	PL-2, PL-8, PM-11, RA-2, SA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-7 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; enterprise architecture policy; procedures addressing information security-related aspects of enterprise architecture development; system development life cycle documentation; results of risk assessment of enterprise architecture; enterprise architecture documentation; enterprise security architecture documentation; other relevant documents or records. **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for developing enterprise architecture; organizational personnel responsible for risk assessment of enterprise architecture; organizational personnel with information security responsibilities.	

PM-7: Enterprise Architecture
Test: Organizational processes for enterprise architecture development; automated mechanisms supporting the enterprise architecture and its development and maintenance.

Table 308. PM-8: Critical Infrastructure Plan

PM-8: Critical Infrastructure Plan	
Control	
The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	
Guidance	
Critical infrastructure protection strategies are based on the prioritization of critical assets and resources. The requirements and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
Related Control Requirement(s):	PM-1, PM-9, PM-11, RA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-8 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; critical infrastructure and key resources protection plan; procedures addressing critical infrastructure plan development and implementation; procedures addressing critical infrastructure plan reviews and updates; records of critical infrastructure plan reviews and updates; other relevant documents or records. **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for developing, documenting, and updating the critical infrastructure and key resources protection plan; organizational personnel with information security responsibilities. **Test:** Organizational processes for developing, documenting, and updating the critical infrastructure and key resources protection plan; automated mechanisms supporting the development, documentation, and updating of the critical infrastructure and key resources protection plan.	

Table 309. PM-9: Risk Management Strategy

PM-9: Risk Management Strategy
Control
The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy as required to address organizational changes.
Guidance

PM-9: Risk Management Strategy	
An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad based and comprehensive.	
Related Control Requirement(s):	RA-3
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-9 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; risk management strategy and policy; procedures addressing development, implementation, review, and update of the risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records. **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for development, implementation, review, and update of the risk management strategy; organizational personnel with information security responsibilities. **Test:** Organizational processes for development, implementation, review and update of the risk management strategy; automated mechanisms supporting the development, implementation, review, and update of the risk management strategy.	

Table 310. PM-10: Security Authorization Process

PM-10: Security Authorization Process
Control
The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program. The Administering Entity's Authorizing Official: a. Grants/denies the Authorization To Operate (ATO) based on the evaluation of security risks; b. Manages the CMS-established Authority to Connect (ATC) process; c. If the organization maintains a system-to-system connection with CMS through an executed Interconnection Security Agreement with CMS, CMS grants/denies the "Authority to Connect"; and d. Grants/denies the authorization to establish system-to-system connections with other external entities.
Guidance
Security authorization processes for information systems and environments of operation require the implementation of an organization-wide risk management process, a risk management framework, and associated

PM-10: Security Authorization Process	
security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.	
Related Control Requirement(s):	CA-6, CA-7
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-10 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; procedures addressing management (i.e., documentation, tracking, and reporting) of the security authorization process; security authorization documents; lists of other documentation about security authorization process roles and responsibilities; security assessment and authorization policy; risk management policy; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records. **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel with security authorization responsibilities for information systems; organizational personnel with risk management responsibilities; authorization officials; business and/or system owners, senior information security officer; organizational personnel with information security responsibilities. **Test:** Organizational processes for security authorization; automated mechanisms supporting the security authorization process.	

Table 311. PM-11: Mission/Business Process Definition

PM-11: Mission/Business Process Definition
Control
The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes, and revises the processes, as necessary, until it defines achievable protection needs.
Guidance
Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. The organization documents its mission/business process definitions and associated information protection requirements in accordance with organizational policy and procedure.

PM-11: Mission/Business Process Definition	
Related Control Requirement(s):	PM-7, PM-8, RA-2

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PM-11 control as described in the control requirements.

Assessment Methods and Objects

Examine: Information security program plan and policy; risk management strategy and policy; procedures addressing security categorization of organizational information and information systems; risk assessment results relevant to determination of mission/business protection needs; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records.

Interview: Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel with mission/business process definition responsibilities; organizational personnel responsible for determining information protection needs for mission/business processes; organizational personnel with security categorization and risk management responsibilities for the information security program; organizational personnel with information security responsibilities.

Test: Organizational processes for defining mission/business processes and their information protection needs.

Table 312. PM-12: Insider Threat Program

PM-12: Insider Threat Program
Control
The organization implements an insider threat program that includes a cross-discipline, insider threat incident-handling team.
Guidance
Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the organization head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs at a minimum prepare department/agency insider threat policies and implementation plans; conduct host-based user monitoring of individual employee activities; provide insider threat awareness training to employees, receive access to information from all offices within the organization (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis; and conduct self-assessments of organizational insider threat posture. Insider threat programs can leverage the incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, because there is compelling evidence that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines.

PM-12: Insider Threat Program	
Related Control Requirement(s):	AT-2, AU-6, AU-7, AU-10, AU-12, CA-7, IA-4, IR-3, IR-4, IR-5, IR-6, MP-7, PE-2, PM-1, PM-14, PS-3, PS-4, PS-5, PS-8, SC-7, SI-4

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization has implemented all elements of the PM-12 control as described in the control requirements.

Assessment Methods and Objects

Examine: Information security program plan and policy; insider threat program documentation; procedures for the insider threat program; risk assessment results relevant to insider threats; list or other documentation on the cross-discipline insider threat incident handling team; risk management policy; procedures addressing incident handling and response; other relevant documents or records.

Interview: Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for the insider threat program; members of the cross-discipline insider threat incident handling team; organizational personnel with information security responsibilities; organizational personnel with risk management responsibilities, organizational personnel with incident response responsibilities.

Test: Organizational processes for implementing the insider threat program and the cross-discipline insider threat incident handling team; automated mechanisms supporting and/or implementing the insider threat program and the cross-discipline insider threat incident handling team.

Table 313. PM-13: Information Security Workforce

PM-13: Information Security Workforce	
Control	
The organization establishes an information security workforce development and improvement program.	
Guidance	
Information security workforce development and improvement programs include, for example, (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals. The information security workforce is trained on the CMS Minimum Acceptable Risk Standards for Exchanges.	
Related Control Requirement(s):	AT-2, AT-3, PS-2

Control Implementation Description:

"Click here and type text"

Assessment Procedure:

PM-13: Information Security Workforce
Assessment Objective Determine if the organization has implemented all elements of the PM-13 control as described in the control requirements.
Assessment Methods and Objects **Examine:** Information security program plan and policy; information security workforce development and improvement program documentation; security workforce development and improvement program procedures; other relevant documents or records. **Interview:** Organizational personnel with risk management responsibilities; organizational personnel with security workforce development program responsibilities; organizational personnel with information security responsibilities. **Test:** Organizational processes for implementing information security workforce development and improvement program; automated mechanisms supporting and/or implementing the information security workforce development and improvement program.

Table 314. PM-14: Testing, Training, and Monitoring

PM-14: Testing, Training, and Monitoring	
Control	
The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: 1. Are developed and maintained; 2. Continue to be executed in a timely manner; and b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	
Guidance	
This control ensures that organizations provide oversight for and coordinate the security testing, training, and monitoring activities conducted organization wide. With the emphasis on continuous monitoring programs, widespread use of common controls, and the implementation of information security across the three tiers of the risk management hierarchy, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. It is necessary to coordinate security training activities across all organizational elements, even though these activities typically focus on individual information systems and specific roles. Current threat and vulnerability assessments inform testing, training, and monitoring plans and activities.	
Related Control Requirement(s):	AT-3, CA-7, CP-4, IR-3, SI-4
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-14 control as described in the control requirements.	
Assessment Methods and Objects **Examine**: Information security program plan and policy; plans for conducting security testing, training, and monitoring activity; organizational procedures addressing development and maintenance of plans for conducting security testing, training, and monitoring activities; risk management strategy; procedures for review of plans for	

PM-14: Testing, Training, and Monitoring
conducting security testing, training, and monitoring activities for consistency with risk management strategy and risk response priorities; results of risk assessments associated with conducting security testing, training, and monitoring activities; evidence that plans for conducting security testing, training, and monitoring activities are executed in a timely manner; other relevant documents or records. **Interview:** Organizational personnel with responsibility for developing and maintaining plans for conducting security testing, training, and monitoring activities; organizational personnel with information security responsibilities. **Test:** Organizational processes for development and maintenance of plans for conducting security testing, training, and monitoring activities; automated mechanisms supporting development and maintenance of plans for conducting security testing, training, and monitoring activities.

Table 315. PM-15: Contacts with Security Groups and Associations

PM-15: Contacts with Security Groups and Associations	
Control	
The organization establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.	
Guidance	
Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
Related Control Requirement(s):	SI-5
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-15 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; risk management strategy; procedures for contacts with security groups and associations; evidence of established and institutionalized contact with security groups and associations; lists or documentation about contact with and/or membership in security groups and associations; other relevant documents or records **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for establishing and institutionalizing contact with security groups and associations; organizational personnel with information security responsibilities; personnel from selected groups and associations with which the organization has established and institutionalized contact. **Test:** Organizational processes for establishing and institutionalizing contact with security groups and associations; automated mechanisms supporting contacts with security groups and associations.	

Table 316. PM-16: Threat Awareness Program

PM-16: Threat Awareness Program	
Control	
The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	
Guidance	
Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations proven effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives and government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.	
Related Control Requirement(s):	PM-12, PM-16
Control Implementation Description: "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has implemented all elements of the PM-16 control as described in the control requirements.	
Assessment Methods and Objects **Examine:** Information security program plan and policy; threat awareness program policy; threat awareness program documentation and procedures; risk assessment results relevant to threat awareness; list or other documentation on the cross-organizational information-sharing capability; other relevant documents or records. **Interview:** Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for the threat awareness program; organizational personnel with responsibility for the cross-organizational information-sharing capability; organizational personnel with information security responsibilities; personnel with whom threat awareness information is shared by the organization. **Test:** Organizational processes for implementing the threat awareness program; organizational processes for implementing the cross-organizational information-sharing capability; automated mechanisms supporting and/or implementing the threat awareness program; automated mechanisms supporting and/or implementing the cross-organizational information sharing capability.	

Part C – Privacy Controls Implementation

1.32 Authority and Purpose (AP)

Table 317. 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.
Guidance
This standard ensures the organization identifies the legal bases that authorize a particular collection of PII, or activity that impacts privacy. The authorities to collect, use, maintain, and share PII must be clearly documented. When documentation appears in an agreement, citation(s) to the applicable law(s), regulation(s), and/or program guidance appear in an Authorities section of the agreement. Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the designated privacy official and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements (CMA). The organization may not create, collect, use, or disclose PII unless in compliance with 45 CFR §155.260. The *CMA between the Centers for Medicare & Medicaid Services and State-based Administering Entities (AE) for the Disclosure of Insurance Affordability Programs Information under the Patient Protection and Affordable Care Act*, establishes the terms, conditions, safeguards, and procedures under which CMS will disclose certain information to the AEs in accordance with the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act (Public Law 111-152), which are referred to collectively as the ACA, amendments to the Social Security Act made by the ACA, and the implementing regulations. Information Exchange Agreements (IEA) between CMS and AEs should also include the legal authority that permits the collection, use, maintenance, and sharing of PII. **For Federal systems:** The authority to collect, use, maintain, or disclose PII is documented in a SORN. The SORN serves as the formal notice to the public, published in the Federal Register, that identifies the purpose for which PII is collected, from whom PII is collected, what type of PII is collected, and how the PII is shared externally. **For non-Federal systems:** The authority to collect, use, maintain, or disclose PII is based on ACA mandate for access to health insurance coverage, and/or based on state statute and regulations. The authority is documented in a PIA. The authority may also be included in other applicable documentation such as the CMA and IEAs as described. CMS provides submission requirements and due dates for privacy agreements in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .

AP-1: Authority to Collect	
Related Control Requirement(s):	AR-2, DM-1, TR-1, TR-2

Control Implementation Description

Cite applicable CMA and IEAs.

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if:

1. The organization determines the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need; and
2. The organization documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

Assessment Methods and Objects

Examine: Legal authority, as applicable, in SORN, PIA, or other documentation such as Privacy Act Statements or CMAs, that permits the collection, use, maintenance, and sharing of PII; PII collection, use, maintenance, and sharing program policy; PII collection, use, maintenance, and sharing program procedures; other relevant documents or records.

Interview: Personnel with responsibilities for determining and documenting legal authority.

Table 318. 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 privacy notices and data sharing agreements.	
Guidance	
Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the designated privacy official and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to PIAs, SORNs, and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.	
Related Control Requirement(s):	AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2

Control Implementation Description

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if the organization provides adequate explanation of the purpose for the collection, creation, use and disclosure of PII prior to collecting information from individuals.

AP-2: Purpose Specification
Assessment Methods and Objects **Examine:** Privacy documents and notices including, but not limited to, PIAs; SORNs; and agreements to collect, use, and disclose PII and Privacy Act Statements provided at the time of collection, such as on forms the AE uses to collect PII. **Interview:** Organizational personnel with responsibilities for determining and documenting permissible purposes for which PII is collected, used, maintained, and shared in privacy documents and notices.

1.33 Accountability, Audit, and Risk Management (AR)

Table 319. 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 AE 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 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, at least biennially.	
Guidance	
The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of a designated privacy official with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The designated privacy official, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls. To further accountability, the designated privacy official develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the designated privacy official. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as PIAs and SORNs. A comprehensive plan may include a baseline of privacy controls selected from this Catalog and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.	
Related Control Requirement(s):	
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization has a designated privacy officialwho is accountable for developing, implementing, and maintaining governance and a strategic privacy program to ensure compliance with all applicable laws	

AR-1: Governance and Privacy Program
and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems; 2. The organization monitors federal (and state as applicable) privacy laws and policy for changes that affect the privacy program; 3. The organization allocates an appropriate budget and staffing to implement and operate the organization-wide program; 4. The organization has operational policies and procedures governing appropriate AE privacy controls for programs, information systems, and technologies involving PII; 5. The organization has a strategic privacy program for implementing all applicable privacy controls, policies, and procedures; 6. The organization monitors and audits to ensure accountability and compliance with identified privacy controls.
Assessment Methods and Objects **Examine:** 1. Documentation designating and describing the authority of the privacy official; 2. Organizational governance and privacy policy; 3. Organization's budget and staffing documentation; 4. Operational policies, procedures, and other governance documents; 5. Organization's privacy program; and 6. Organization's monitoring and auditing policies and procedures. **Interview:** 1. Organization's designated privacy official; 2. Other organizational personnel, as designated by privacy official, with responsibility for governance documents and privacy program implementation.

Table 320. 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, and other AE activities that pose a risk to the privacy of PII.
Guidance
Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. AEs need to develop a privacy risk assessment framework and employ tools and processes for managing risk to include, but not limited to, conducting a Privacy Impact Assessment (PIA). The PIA is both a process and the documentation of the outcome of the privacy risk assessment. AEs are required to complete and submit the ACA Health Insurance Administering Entity PIA to CMS annually or when a system or program change occurs that may have an impact on the PII that is collected, created, used, or disclosed. Examples of scenarios when the AEs should update PIAs include, but are not limited to, when there are significant changes to the Administering Entity privacy program or IT systems, when new PII data elements are added to the system, when existing PII data elements are to be removed from the system, or when there are changes to data-sharing policies or agreements that may change the AE's privacy risk profile.

AR-2: Privacy Impact and Risk Assessment	
CMS provides submission requirements and due dates for the PIA in the MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table located at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Related Control Requirement(s):	SE-2
Control Implementation Description *** Note: The Privacy Impact Assessment is a required artifact. «Click here and type text.]»	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization documents and implements a privacy risk assessment process that assess privacy risks to individuals resulting from collection, sharing, storing, transmitting, use, and disposal of PII; and 2. The organization conducts privacy impact assessments for information systems, programs, and other activities that pose a privacy risk.	
Assessment Methods and Objects **Examine:** 1. Documentation describing the AE privacy risk assessment process; 2. Documentation of privacy risk assessment(s) conducted by the organization; and 3. Privacy risk management planning policy, procedures addressing privacy impact assessments on the system, and other relevant documents or records. **Interview:** 1. Organization's designated privacy official, or other organizational personnel, as designated by the privacy official, with responsibility for AE privacy risk assessment.	

Table 321. AR-3: Privacy Requirements for Contractors and Service Providers

AR-3: Privacy Requirements for Contractors and Service Providers
Control
The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers, and b. Includes privacy requirements in contracts and other acquisition-related documents.
Guidance
Contractors and providers include, but are not limited to, information providers, information processors, and other organizations that provide information system development, information technology services, consumer assistance, AE business functions, and other outsourced applications, roles, and functions. Organizations consult with legal counsel, the designated privacy official, and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. **Specific to Non-Exchange Entities:** Regulatory provisions at 45 CFR §155.260 describe how Marketplace privacy and security requirements apply to non-Exchange entities (NEE). 45 CFR §155.260(b)(1) defines NEEs as any individual or entity that: (i) gains access to personally identifiable information submitted to an Exchange; or (ii) collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.

AR-3: Privacy Requirements for Contractors and Service Providers	
Specific to Marketplaces: : §155.260(b)(2) requires that, before any person or entity becomes a NEE, the Marketplace must execute with that person or entity a contract or agreement that includesprovisions that are specified at §155.260(b)(2)(i)-(v). These provisions must: 1. Describe the functions the NEE is to perform; 2. Bind the NEE to comply with privacy and security requirements adopted in accordance with paragraph §155.260(b)(3), specifically listing or incorporating those privacy and security standards and obligations; 3. Require the NEE to monitor, periodically assess, and update its security controls and related system risks to ensure their continued effectiveness; 4. Require the NEE to inform the *[Marketplace]* of any change in its administrative, technical, or operational environments defined as material within the contract; and 5. Require the NEE to bind any downstream entities to the same privacy and security standards and obligations to which the NEE has agreed in its contract or agreement with the *[Marketplace]*. §155.260(b)(3) further requires that, when collection, use, or disclosure is not otherwise required by law, the privacy and security standards to which a Marketplace binds a NEE must be consistent with the principles and requirements listed in §155.260(a)(1)-(6), including, but not limited to, being at least as protective as the standards the Marketplace has established and implemented for itself in compliance with §155.260(a)(3). The standards to which a Marketplace binds a NEE also must adhere to the requirements listed at §155.260(c),(d),(f), and (g), and must take into specific consideration: 1. The environment in which the NEE operates; 2. Whether the standards are relevant and applicable to the NEE's duties and activities in connection with the Marketplace, and 3. Any existing legal requirements to which the NEE is bound in relation to its administrative, technical, and operational controls and practices, including but not limited to. its existing data handling and information technology processes and protocols. **Specific to Medicaid and CHIP:** While Medicaid/CHIP is itself an NEE, the organization must follow the guiance in §155.260(b)(2) stated above when executing an agreement with another NEE in performing a function for the Medicaid/CHIP agency.	
Related Control Requirement(s):	AR-1, AR-5, SA-4
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization has established privacy roles, responsibilities, and access requirements for AE-related contractors and service providers, and 2. The organization includes privacy requirements in contracts and other agreements with contractors, services providers, and other downstream entities.	
Assessment Methods and Objects **Examine:** 1. Organization's policies and procedures defining privacy roles, responsibilities, and access requirements for contractors, service providers, and other downstream entities; and 2. Privacy requirements included in organization's contracts and other agreements. **Interview:** 1. Organization's designated privacy official; and 2. Other organizational personnel, as designated by the privacy official, with responsibilities for AE-related contract(s) and agreement(s).	

Table 322. AR-4: Privacy Monitoring and Auditing

AR-4: Privacy Monitoring and Auditing
Control
The organization: a. Monitors and audits privacy controls and internal privacy policy as required to ensure effective implementation; and b. Complies with HHS privacy oversight monitoring and auditing policies and procedures.
Guidance
To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in this document, organizations assess whether they: 1. Implement a process to embed privacy considerations into the life cycle of PII, programs, information systems, mission/business processes, and technology; 2. Monitor for changes to applicable privacy laws, regulations, and policies; 3. Track programs, information systems, and applications that collect and maintain PII to ensure compliance; 4. Ensure that access to PII is only on a need-to-know basis; and 5. Ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s). Organizations also: 1. Implement technology to audit for the security, appropriate use, and loss of PII; 2. Perform reviews to ensure physical security of documents containing PII; 3. Assess contractor compliance with privacy requirements; 4. Ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected; 5. Monitors and audits privacy controls and internal privacy policy as required to ensure effective implementation; and 6. Complies with HHS privacy oversight monitoring and auditing policies and procedures. 7. The organization's designated privacy official coordinates monitoring and auditing efforts with information security officials and ensures the results are provided to senior managers and oversight officials. The organization should coordinate the privacy control monitoring and auditing processes and the security control continuous monitoring process required by CA-7, Continuous Monitoring. Per 45 CFR §155.280 – Oversight and monitoring of privacy and security requirements, the Federally-facilitated Exchanges and Non-Exchange entities associated with the Federally-facilitated Exchange are subject to HHS oversight and monitoring for compliance with the standards established by the Federally-facilitated Exchange, and State-based Exchanges are subject to HHS oversight and monitoring for compliance with the privacy and security standards that the State-based Exchange establishes, while the non-Exchange entities that are associated with State-based Exchanges are subject to the oversight and monitoring of the State-based Exchanges with which they are associated. **Specific to SBMs:** In addition, 45 CFR §155.1200(c) states, "The State [Marketplace] must engage an independent qualified auditing entity which follows generally accepted governmental auditing standards (GAGAS) to perform an annual independent external financial and programmatic audit and must make such information available to HHS for review…" The SBM privacy and security program is included as a component of the annual independent external financial and programmatic audit to ensure the State Marketplace's compliance with the policies and procedures established and implemented under §155.260(a)(3).

AR-4: Privacy Monitoring and Auditing	
Related Control Requirement(s):	AR-6, 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"

Assessment Procedure:

Assessment Objective

Determine if: the organization monitors and audit privacy controls and internal privacy policy, as required, to ensure effective implementation.

Assessment Methods and Objects

Examine:

1. Organization's privacy monitoring policies and procedures describing regular internal assessments and/or third-party audits for AE-related privacy controls;
2. Most recently completed assessment(s) and/or third-party audit report(s);
3. Organization's policies and procedures for assessing contractor compliance with AE-related privacy requirements in contract provisions; and
4. Records of any corrective actions identified as part of assessment process and correction of audit findings.

Interview:

1. Organization's designated privacy official and/or chief privacy officer;
2. Other organizational personnel, as designated by privacy official, with responsibility for privacy assessments and audits; and
3. Third-party auditors as necessary.

Table 323. AR-5: Privacy Awareness and Training

AR-5: Privacy Awareness and Training
Control
The organization: a. Develops, implements, and updates a comprehensive AE privacy training and awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures; b. Administer basic privacy training at least annually, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII at least annually; and c. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually.
Guidance
Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy compliance. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as PIAs or SORNs for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training.

AR-5: Privacy Awareness and Training	
Organizations should consider combining the privacy and security awareness and training programs and control requirements. Organizations should determine how to incorporate privacy awareness and training content into the controls the organization is required to implement under security controls AT-2 – *Security Awareness Training*, AT-3 – *Role-Based Security Training*, and AT-4 – *Security Training Records*.	
Related Control Requirement(s):	AR-3, AT-2, AT-3, AT-4, TR-1
Control Implementation Description "Click here and type text"	
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.	

Table 324. AR-6: Privacy Reporting

AR-6: Privacy Reporting
Control
The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.This control does not apply to non-Federal entities.
Guidance
This control does not apply to non-Federal entities. This control is meant for Department-level reporting to OMB and Congress about the Department's privacy program. Through internal and external privacy reporting, this standard ensures the organization promotes accountability and transparency in its privacy operations. Reporting helps the organization to: 1. Determine progress in meeting privacy compliance requirements and controls, 2. Compare performance across organizations,

AR-6: Privacy Reporting	
3. Identify vulnerabilities and gaps in policy and implementation; and 4. Identify models for success. The organization's designated privacy official consults with legal counsel, where appropriate, to ensure organizations meet all applicable privacy reporting requirements.	
Related Control Requirement(s):	
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization develops privacy reports to the OMB, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance; 2. The organization disseminates privacy reports to the OMB, Congress, and other oversight bodies, as appropriate, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance; and 3. The organization updates privacy reports within the time period specified by specific statutory and regulatory privacy program mandates but no less than within every 365 days.	
Assessment Methods and Objects **Examine:** Reports to OMB, Congress, and other oversight bodies, as appropriate; reports to senior management and personnel with responsibility for monitoring privacy program progress and compliance; other relevant documents or records. **Interview:** The privacy officer, senior management, and personnel with responsibility for monitoring privacy program reporting progress.	

Table 325. AR-7: Privacy-enhanced System Design and Development

AR-7: Privacy-enhanced System Design and Development
Control
The organization designs information systems that support privacy with automated privacy controls.
Guidance
To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII. By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the 45 CFR §155.260, the Privacy Act (if applicable) and the organization's privacy policy. The organization should review and adhere to its Control Implementation Description for the SA-3 – System Development Life Cycle control when implementing this control.

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"

Assessment Procedure:

Assessment Objective

Determine if: the organization designs information system to support privacy by automating privacy controls related to collection, use, maintenance, and disclosure of PII.

Assessment Methods and Objects

Examine: Information system design documentation; other relevant documents or records.

Interview: Organizational personnel with responsibilities for information system design.

Table 326. 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 five 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.

Guidance

The designated privacy official periodically consults with managers of the organization systems of record to ensure the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. §552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals.

Related Control Requirement(s):	IP-2, AU-2, AU-3, AU-11

Control Implementation Description

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if:

1. The organization accurately documents and accounts for all disclosures of PII, and
2. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
3. Makes the accounting of disclosures available to the person named in the record upon request.

AR-8: Accounting of Disclosures
Assessment Methods and Objects **Examine:** 1. Documentation of accounting of disclosures the AE maintains; 2. Retention policy for the disclosure of records; 3. Retention policy for making disclosures available to the person named in the record upon request; and 4. Current legal agreements concerning the sharing of data. **Interview:** Organizational personnel with responsibilities for maintaining the accounting of disclosures.

1.34 Data Quality and Integrity (DI)

Table 327. 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 as directed by the HHS Data Integrity Board; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	
Guidance	
Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under Federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals. When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.	
Related Control Requirement(s):	AP-2, DI-2, DM-1, IP-3 SI-10
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information; 2. The organization collects PII directly from individual to the greatest extent practicable; 3. The organization validates and corrects any inaccurate or outdated PII; and 4. The organization issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	
Assessment Methods and Objects **Examine:** 1. Procedures (automated or manual) that are in place to confirm the quality, utility, objectivity, and integrity of PII; 2. Privacy policy, privacy program plan, privacy program procedures; and 3. Guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	

Table 328. D-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.	
Guidance	
See DI-1 control guidance.	
Related Control Requirement(s):	AP-2, DI-2, DM-1, IP-3, SI-10
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization requests that the individual or individual's authorized representative validate PII during the collection process.	
Assessment Methods and Objects **Examine:** Organization privacy policy; privacy program plan; privacy program procedures; PII validation procedures; other relevant documents or records.	

Table 329. DI-1 (2): Re-validate PII

D1-1 (2): Re-validate PII	
Control	
The organization requests the individual or the individual's authorized representative revalidate that PII collected is still accurate.	
Guidance	
See DI-1 control guidance.	
Related Control Requirement(s):	AP-2, DI-2, DM-1, IP-3, SI-10
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: the organization requests the individual or individual's authorized representative revalidate that PII collected is still accurate as directed by the HHS Data Integrity Board.	
Assessment Methods and Objects **Examine:** 1. Organization's privacy policy, privacy program plan and privacy program procedures that have been implemented to re-validate PII; and 2. Organization's PII validation procedures.	

Table 330. DI-2: Data Integrity and Data Integrity Board

DI-2: Data Integrity and Data Integrity Board	
Control	
The organization: a. Document processes and procedures to ensure the integrity of PII through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational CMAs and to ensure those agreements comply with the computer matching provisions of the Privacy Act.	
Guidance	
Organizations conducting or participating in CMAs with other organizations regarding applicants for and recipients of financial assistance or payments under Federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the designated privacy official. The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under CMAs. **Specific to all non-Federal Entities:** *Non-Federal entities are not required to implement this control*.	
Related Control Requirement(s):	AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization documents processes to ensure the integrity of PII through existing security controls; and 2. The organization establishes a Data Integrity Board when appropriate to oversee organizational CMAs and to ensure those agreements comply with the computer matching provisions of the Privacy Act.	
Assessment Methods and Objects **Examine:** Organization PII integrity policy; PII integrity program plan; PII integrity process and procedures; information security plan; other relevant documents or records.	

Table 331. DI-2 (1): Publish Agreements on Website

DI-2 (1): Publish Agreements on Website	
Control	
The organization publishes CMAs on its public website. **Non-Federal entities are not required to implement this control.**	
Guidance	
This is a “fully inherited” control. CMS is responsible for publishing the FFM CMA and other agreements on its public website.	
Related Control Requirement(s):	AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2

DI-2 (1): Publish Agreements on Website
Control Implementation Description "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if CMS publishes CMAs for the FFM on its public website.
Assessment Methods and Objects **Examine:** Organization CMAs; other relevant documents or records.

1.35 Data Minimization and Retention (DM)

Table 332. 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 periodically review the holdings, within every 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.	
Guidance	
Organizations take appropriate steps to ensure the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the designated privacy official and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose. Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with National Archives and Records Administration (NARA) NIST SP 800-122 provides guidance on anonymization retention schedules. By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice.	
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"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; 2. The organization 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 3. The organization conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, within every 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.	

DM-1: Minimization of Personally Identifiable Information
Assessment Methods and Objects **Examine**: 1. Organization privacy data minimization and retention policy; 2. Privacy data minimization and retention program plan; 3. Privacy data minimization and retention program procedures; 4. PII holding evaluation and review documentation; and 5. Inventory of PII. **Interview:** Individuals responsible for conducting the review of PII holdings and maintaining the inventory of PII.

Table 333. DM-1 (1): Minimization of PII/Locate/Remove/Redact/Anonymize PII

DM-1 (1): Minimization of PII/Locate/Remove/Redact/Anonymize PII	
Control	
The organization, where feasible and within the limits of technology, 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.	
Guidance	
NIST SP 800-122 provides guidance on anonymization.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization, where feasible and within the limits of technology, 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.	
Assessment Methods and Objects **Examine:** Organization privacy data anonymization and de-identification policy; privacy data anonymization and de-identification policy procedures; other relevant documents or records.	

Table 334. DM-2: Data Retention and Disposal

DM-2: Data Retention and Disposal
Control
The organization: a. Retains each collection of PII for the minimum allowable time period necessary 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

DM-2: Data Retention and Disposal
c. Uses legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Guidance

NARA provides retention schedules that govern the disposition of Federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper. Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media.

Specific to SBMs: 45 CFR §155.1210 Maintenance of Records states the SBMs must maintain and ensure contractors, subcontractors, and agents maintain certain documents and records for 10 years. These documents and records (whether paper, electronic, or other media) and other evidence of accounting procedures and practices, must be sufficient to: accommodate periodic auditing of financial records, and enable HHS or its designee(s) to inspect facilities, or otherwise evaluate the SBM's compliance with federal standards. The requirement further states that the records include, at a minimum, the following:

1. Information concerning management and operation of the SBM's financial and other record keeping systems;
2. Financial statements;
3. Any financial reports filed with other federal programs or state authorities;
4. Data and records relating to the SBM's eligibility verifications and determinations, enrollment transactions, appeals, and plan variation certifications; and
5. Qualified health plan (QHP) contracting (including benefit review) data and consumer outreach and Navigator grant oversight information.

SBMs are required to maintain a record and data retention schedule. Other federal or state laws or regulations may require, or allow, data within this record set to be destroyed earlier than the retention period required by §155.1210. However, SBMs must adhere to the record retention timeframes as described in the Marketplace regulations.

Specific to Medicaid/CHIP AEs: Medicaid and CHIP performing ACA Administering Entity functions must comply with the records retention requirements that apply to SBMs as well as Records Retention requirements specified in 42 CFR 431.17 - Maintenance of records, based on section 1902(a)(4) of the Social Security Act.

For Federal Systems: NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.

Related Control Requirement(s):	AR-4, AU-11, DM-1, MP-1, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1

Control Implementation Description

"Click here and type text"

Assessment Procedure:

Assessment Objective

Determine if:

1. The organization retains each collection of PII for minimum allowable time period necessary to fulfill the purpose(s) identified in the notice or as required by law;

DM-2: Data Retention and Disposal
2. The organization disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with an approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and 3. The organization uses legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
Assessment Methods and Objects **Examine:** 1. Organization PII retention policy; PII retention procedures; organization PII disposal policy; PII disposal procedures; other relevant documents or records; and 2. A sample of destruction records, if applicable. **Interview:** Staff to ensure documented procedures are implemented in a consistent manner throughout the organization.

Table 335. DM-2 (1): Data Retention and Disposal/System Configuration

DM-2 (1): Data Retention and Disposal/System Configuration	
Control	
The organization configures information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under a record retention schedule.	
Guidance	
See DM-2 control guidance.	
Related Control Requirement(s):	AR-4, AU-11, DM-1, MP-1, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.	
Assessment Methods and Objects **Examine:** Information system configuration documentation; information system PII audit records; other relevant documents or records.	

Table 336. 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.
Guidance

DM-3: Minimization of PII Used in Testing, Training, and Research	
If PII must be used for research, AEs take measures to minimize any associated risks and to authorize the use of, and limit the amount of, PII for these purposes. Organizations consult with the designated privacy official and legal counsel to ensure the use of PII is compatible with the original purpose for which it was collected. PII should not be used for testing and training for any AE functions. State laws may also govern the use of PII for other functions.	
Related Control Requirement(s):	
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization develops policies and procedures that minimize the use of PII for testing, training, and research; and 2. The organization implements controls to protect PII used for testing, training, and research.	
Assessment Methods and Objects **Examine:** Organization policies concerning the use of PII used for testing, training, and research; procedures concerning the use of PII used for testing, training, and research; controls used to protect PII used for testing, training, and research; other relevant documents or records.	

Table 337. DM-3 (1): Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques

DM-3 (1): Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques	
Control	
The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.	
Guidance	
Organizations can minimize risk to privacy of PII by using techniques such as de-identification or randomly generate data to match PII characteristics.	
Related Control Requirement(s):	
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.	

DM-3 (1): Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques
Assessment Methods and Objects **Examine:** Organization policies to minimize the risk of using PII for testing, training, and research; procedures to minimize the risk of using PII for testing, training, and research; techniques used to minimize the risk of using PII for testing, training, and research; other relevant documents or records. **Interview:** Personnel tasked with implementation and compliance

1.36 Individual Participation and Redress (IP)

Table 338. 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 before its collection; 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 before any new uses or disclosures of previously collected PII; and d. Ensures individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.
Guidance
Consent is fundamental to the participation of individuals in the decision-making process for the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals with appropriate notice of the purposes of the PII collection or technology used and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices. Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. For example, the Federal Trade Commission's Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization. AEs should develop and implement processes for collecting consent from individuals who comply with state law or, where applicable, defer to federal law governing consent. Public notices describing permissible uses of PII appear on public notices and websites issued by the AE. The submission of application for health insurance enrollment automatically gives consent.
Related Control Requirement(s): AC-2, AP-1, TR-1, TR-2
Control Implementation Description "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if: 1. The organization provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;

IP-1: Consent
2. The organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; 3. The organization obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and 4. The organization ensures individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.
Assessment Methods and Objects **Examine:** Organization policy that authorizes the collection, use, maintaining, and sharing of PII prior to its collection; procedures to authorize the collection, use, maintaining, and sharing of PII prior to its collection; other relevant documents or records.

Table 339. IP-1 (1): Mechanism Supporting Itemized or Tiered Consent

IP-1 (1): Mechanism Supporting Itemized or Tiered Consent	
Control	
The organization implements mechanisms to support itemized or tiered consent for specific uses of data.	
Guidance	
Organizations can provide, for example, individuals' itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that organizational operations comply with individual choices.	
Related Control Requirement(s):	AC-2, AP-1, TR-1, TR-2
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: the organization implements mechanisms to support itemized or tiered consent for specific uses of data.	
Assessment Methods and Objects **Examine:** Organization mechanisms implemented to support itemized or tiered consent for specific uses of data; other relevant documents or records.	

Table 340. 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

IP-2: Individual Access	
d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.	
Guidance	
Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The organization's designated privacy official is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate. Heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access information compiled in reasonable anticipation of a civil action or proceeding. **Specific to Federal systems:** Any individual may request access to any record pertaining to him that is maintained in a federal system of record. An individual making a request for access to a record shall address his request to the responsible Department official and shall verify his identity. At the time the request is made, the individual shall specify which systems of records s/he wishes to have searched and the records to which s/he wishes to have access. The individual may also request that copies be made of all or any such records. An individual shall also provide the responsible Department official with sufficient particulars to enable such official to distinguish between records on subject individuals with the same name. The necessary particulars are set forth in the notices of systems of records. **Specific to State-based Administering Entities:** A state agency (Medicaid/CHIP) or State-based Marketplace that collects personally identifiable information must adhere to state laws that may require granting access to the records or information maintained in the state agency's records similar to the Privacy Act's requirements and the DHHS Privacy Act regulations.	
Related Control Requirement(s):	AR-8, IP-3, TR-1, TR-2
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. Organization has processes and procedures enabling individuals' access to their PII that is maintained in its system(s) of records; 2. The organization publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; 3. The organization publishes access procedures ; and 4. The organization adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.	
Assessment Methods and Objects **Examine:** 1. Organization policy providing individuals access to their PII maintained in system(s) of records; 2. Procedures providing individuals access to their PII maintained in system(s) of record; 3. Published rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; and 4. Access procedures in SORNs or privacy notice and/or other relevant documents or records. **Interview:** Staff on how organization adheres to Privacy Act requirements and OMB policies and guidance for processing of Privacy Act requests.	

Table 341. IP-3: Redress

IP-3: Redress	
Control	
The organization: a. Provide information to individuals concerning how to contact the relevant organization to have inaccurate PII maintained by that organization corrected or amended, as appropriate; and b. Establish 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.	
Guidance	
Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality, especially with respect to business functions where inaccurate data may result in inappropriate decisions or denial of benefits or services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate. To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information. Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information.	
Related Control Requirement(s):	IP-2, TR-1, TR-2, UL-2
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and 2. The organization establishes a process for disseminating corrections or amendments of the PII 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.	
Assessment Methods and Objects **Examine:** 1. Process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; 2. Process for disseminating corrections or amendments of the PII to other authorized users of the PII; and 3. Process for notifying affected individuals that their information has been corrected or amended. **Interview:** Personnel tasked to develop redress policies and processing corrections.	

Table 342. 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.	
Guidance	
Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints, and are easy to use. Complaint management processes include tracking mechanisms to ensure all complaints received are reviewed and appropriately addressed in a timely manner.	
Related Control Requirement(s):	AR-6, IP-3
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization has processes and procedures for receiving and responding to complaints from individuals about organizational privacy practices.	
Assessment Methods and Objects **Examine:** 1. The process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices; other relevant documents or records; and 2. Any complaints submitted by individuals concerning their PII (including use, disclosure, or inaccuracies), the associated response and mitigation steps implemented to resolve and prevent the situation from occurring again in the future.	

Table 343. IP-4 (1): Complaint Management/Response Times

IP-4 (1): Complaint Management/Response Times	
Control	
The organization responds to complaints, concerns, and questions from individuals within an *[organization-defined]* time period.	
Guidance	
See IP-4 control guidance.	
Related Control Requirement(s):	AR-6, IP-3

IP-4 (1): Complaint Management/Response Times
Control Implementation Description "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if: the organization responds to complaints, concerns, or questions from individuals within a defined time period.
Assessment Methods and Objects **Examine:** The process for responding to complaints, concerns, or questions from individuals; other relevant documents or records.

1.37 Security (SE)

Table 344. SE-1: Inventory of Personally Identifiable Information

SE-1: Inventory of Personally Identifiable Information	
Control	
The organization: a. Establishes, maintains, and updates within 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 privacy official or information security official to support the establishment of information security requirements for all new or modified information systems containing PII.	
Guidance	
The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Volume III of the Minimum Acceptable Risk Standards for Exchanges (MARS-E) document suite (Version 2.0), *Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*, and to mitigate risks of PII exposure. As one method of gathering information for PII inventories, organizations may extract the following information elements from PIA for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII. AEs need to develop an inventory of PII to correlate to the PII data elements documented within the PIA. The PII inventory identifies: (i) the name and acronym for each program and system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII as collected, used, maintained, or shared by that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed.	
Related Control Requirement(s):	AR-1, AR-4, AR-5, AT-1, DM-1, PM-5
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization establishes, maintains, and updates, within every 365 days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and 2. The organization provides each update of the PII inventory to the organization's designated privacy official and the CISO to support the establishment of information security requirements for all new or modified information systems containing PII.	
Assessment Methods and Objects **Examine:** Organizational policies, procedures and PII inventory, inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII.	

Table 345. SE-2: Privacy Incident Response

SE-2: Privacy Incident Response	
Control	
The organization: a. Develops and implements a Privacy Incident Response Plan; b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan; and c. Follows current CMS Incident Reporting requirements for reporting incidents to oversight organizations as defined in the incident handling documents available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ .	
Guidance	
In contrast to the Incident Response (IR) family in the security controls, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to PII. The organization Privacy Incident Response Plan is developed under the leadership of the designated privacy official. The plan includes: 1. The establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; 2. A process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly; 3. A privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; 4. Internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the organization's designated privacy official, consistent with organizational incident management structures; and 5. Internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Organizations should work toward integrating the Privacy Incident Response Plan with their Security Incident Response Plan.	
Related Control Requirement(s):	AR-1, AR-4, AR-5, AR-6, AU-1 through AU-14, IR-2, IR-4, IR-6, IR-8, RA-1
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization develops and implements a Privacy Incident Response Plan; and 2. The organization provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.	
Assessment Methods and Objects **Examine:** Organization Privacy Incident Response Plan; privacy incident response procedures; other relevant documents or records.	

1.38 Transparency (TR)

Table 346. 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. 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. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before, or as soon as practicable after the change.	
Guidance	
Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations the organization has addressed in implementing its information practices. General public notice and direct notice to individuals may be provided through a variety of means including SORNs, PIAs, or in a website privacy policy, as required by applicable law and policy. The organization's designated privacy official is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. **Specific to FFMs:** General public notice is provided through SORNs. The Federal Privacy Act also requires Federal organizations to provide direct notice to individuals via Privacy Act Statements on the paper and electronic forms used to collect PII, or on separate forms that individuals can retain. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices.	
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"	
Assessment Procedure:	
Assessment Objective Determine if:	

TR-1: Privacy Notice
1. The organization provides effective notice to the public and to individuals regarding: – Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; – Authority for collecting PII; – The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and – The ability to access and have PII amended or corrected if necessary. 2. The organization describes: – The PII the organization collects and the purpose(s) for which it collects that information; – How the organization uses PII internally; – Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; – Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; – How individuals may obtain access to PII; and – How the PII will be protected. 3. The organization revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before, or as soon as practicable after the change.
Assessment Methods and Objects **Examine:** Public notice regarding individual privacy and PII; other relevant documents or records.

Table 347. TR-1 (1): Real-time or Layered Notice

TR-1 (1): Real-time or Layered Notice	
Control	
The organization provides real-time and/or layered notice to individuals at the time when any PII is collected.	
Guidance	
Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed and specific information.	
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"	
Assessment Procedure:	
Assessment Objective Determine if the organization provides real-time and/or layered notice when it collects PII.	
Assessment Methods and Objects **Examine:** Evidence of real-time and/or layered notice to individuals when any PII is collected; other relevant documents or records.	

Table 348. TR-2: System of Records Notices and Privacy Act Statements

TR-2: System of Records Notices and Privacy Act Statements	
Control	
The organization: a. Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII; b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected. **Non-Federal systems are not required to implement this control.** State-based systems must adhere to state laws that may require publication of a notice similar to the federal SORN and Privacy Act Statement.	
Guidance	
Specific to SBMs: SBMs are not required to implement this control. SBMs must adhere to state laws that may require publication of a notice similar to the federal SORN and Privacy Act Statement. **Specific to FFMs:** The organization issues SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. A Privacy Act Statement provides notice of: 1. The authority of the AE to collect PII; 2. Whether providing PII is mandatory or optional; 3. The principal purpose(s) for which the PII is to be used; 4. The intended disclosure (routine uses) of the PII; and 5. The consequences of not providing all, or some portion of, the PII requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys).	
Related Control Requirement(s):	DI-2
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII; 2. The organization keeps SORNs current; 3. The organization includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected; and 4. The Privacy Act Statement is provided as specified.	
Assessment Methods and Objects **Examine:** Organization SORN(s); Privacy Act Statements on forms that collect PII; Privacy Act Statements on separate forms for individuals; other relevant documents or records.	

Table 349. TR-2 (1): Public Website Publication

TR-2 (1): Public Website Publication	
Control	
The organization publishes SORNs on its public website. **Non-Federal systems are not required to implement this control.** State-based systems must adhere to state laws that may require publication of a notice similar to the federal SORN and Privacy Act Statement.	
Guidance	
The organization publishes SORNs on its public website.	
Related Control Requirement(s):	
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization publishes SORNS on its public website.	
Assessment Methods and Objects **Examine:** Organization SORN(s) on public website; other relevant documents or records.	

Table 350. 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 practices are publicly available through organizational websites or otherwise.	
Guidance	
Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, PIAs, SORNs, privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.	
Related Control Requirement(s):	AR-6

TR-3: Dissemination of Privacy Program Information
Control Implementation Description "Click here and type text"
Assessment Procedure:
Assessment Objective Determine if: 1. The organization ensures the public has access to information about its privacy activities and is able to communicate with its designated privacy official; and 2. The organization ensures its privacy practices are publicly available through organizational websites or otherwise.
Assessment Methods and Objects **Examine:** Organization SORN(s) on public website; posted privacy practices and policies; other relevant documents or records.

1.39 Use Limitation (UL)

Table 351. UL-1: Internal Use

UL-1: Internal Use	
Control	
The organization (each AE) uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	
Guidance	
Organizations take steps to ensure they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the organization's designated privacy official and, where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII. **Specific to FFMs:** These organizations further ensure PII is used internally in a manner compatible with uses identified in §155.260(a) and the Privacy Act. These steps include monitoring and auditing organizational uses of PII, and training personnel on the authorized uses of PII.	
Related Control Requirement(s):	AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2
Control Implementation Description "Click here and type text"	
Assessment Procedure:	
Assessment Objective Determine if the organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	
Assessment Methods and Objects **Examine:** Organization privacy policy; organization privacy practices; other relevant documents or records.	

Table 352. 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 (CMA), 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.

UL-2: Information Sharing with Third Parties	
Guidance	
The organization's designated privacy official and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their PIAs, SORNs, website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.	
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"	
Assessment Procedure:	
Assessment Objective Determine if: 1. The organization shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes; 2. The organization where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, 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; 3. The organization 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 4. The organization 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.	
Assessment Methods and Objects **Examine:** Organization privacy policy; organization privacy practices; Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, CMAs, or similar agreements with third parties (such as non-Marketplace entities); system configuration; audit records; training records; data matching and sharing agreements with agencies administering Medicaid, CHIP, or the Basic Health Program for the exchange of eligibility information; other relevant documents or records.	

Part D – Attachments

The following System Security Plan (SSP) attachments represent documentation that may be developed and maintained as separate documents but must be included with the SSP for evaluation. Most of these attachments are associated with the configuration management (CM) control family and can be also referenced in the configuration management plan. Maintaining these documents as attachments facilitates version control of all the related materials. These attachments should be updated if there is a major change in the security profile. At a minimum, the SSP must contain the following:

- **Attachment A –** 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. This attachment should be labeled as Attachment A – SSP Equipment List.
- **Attachment B –** 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. This attachment should be labeled as Attachment B – SSP Software List.
- **Attachment C –** This attachment contains the detailed configuration settings that satisfy the required CMS baseline configurations. These settings should be consistent with the requirements of CM-2 and CM-6 security controls and associated implementation standards. This attachment should be labeled as Attachment C – SSP Detailed Configuration Settings.
- **Attachment D – SSP Acronyms and Abbreviations.** This attachment contains the acronyms and abbreviations used in the SSP that are not defined in MARS-E, and is provided for additional clarity.
- **Attachment E – SSP Glossary.** This attachment contains the glossary of terms used in the SSP that are not defined in MARS-E, and is provided for additional clarity.

Please list any additional attachments here:

- SSP Attachment *x* –

Attachment A: Sample SSP Equipment List

Host Name	IP Address	CPU	Memory	Application	OS
Prod_PresentationServer	10.10.*.*	2	8 Gig	Production Web Server	Windows 2012
Prod_ApplicationServer		2	4 Gig	Production Application Server	
Prod_DB1		2	4 Gig	Production Database Server	Oracle

Attachment B: Sample SSP Software List

Software Application	Version	Function
Windows Server 2012	R2	Enterprise Server
MySQL Enterprise		Enterprise Database
Apache	2.4.16	HTTP Server
Google Search Appliance (GSA)	7.2	Search Engine
Oracle	11g	Enterprise Database

Attachment C: Sample Detailed Configuration Setting Standards

Component	Configuration Setting	Security Control
SQL Server	Sysadmin and dba SQL server logins should have expiring passwords and the option “CHECK Expiration” should be set on. For application level IDs, this option should be turned off and the passwords manually scheduled/changed every 60 days.	IA-5
Web Server	Configure web server to require the use of FIPS-approved cryptographic algorithms. FIPS-compliant algorithms enable strong encryption, hashing, and signing.	SC-13
Database server	Enable the AUDIT_SYS_OPERATIONS parameter to allow the full auditing of operations issued by user SYS, and users connecting with SYSDBA or SYSOPER privileges.	AU-2 AU-6
Database Server	Set the parameter FAILED_LOGIN_ATTEMPTS to 3 during a 15-minute time.	AC-7
Windows Servers	Ensure Windows servers are configured to require use of FIPS-compliant algorithms.	SC-13
Network Devices	Implement session timeouts on all administrative ports for a timeout value set to 15 minutes or less.	AC-11
Windows Servers	Ensure the built-in guest and administrator accounts are renamed or disabled.	AC-2
SQL Server	For all DBMS accounts using SQL Server logins, set the ‘CHECK_POLICY’ Option to ON for all SQL Authenticated Logins.accounts for password complexity checking.	IA-5
HTTP Server	Set the SECURE flag on all cookies that are used for transmitting sensitive data when accessing content over HTTPS.	SC-8

Attachment D: SSP Acronyms and Abbreviations

Term	Definition
ACA	Patient Protection and Affordable Care Act of 2010
CIO	Chief Information Officer
CISO	Chief Information Security Officer
FTI	Federal Tax Information
HHS	Department of Health and Human Services
MA	Major Application
IRC	Internal Revenue Code
IRS	Internal Revenue Service
	When the Acronym list is complete, turn off the gridline view by clicking "View Gridlines" on the Table Layout ribbon.

Term	Definition

Attachment E: SSP Glossary

[Term]	Define the term by starting with an incomplete sentence that does not repeat the term being defined.
	To insert or delete a row, right-click the desired row and select from the options available when you point to Insert: Insert Above, Insert Below, or Delete Row. The Table Layout ribbon offers the same choices.
	When the Glossary is complete, turn off the gridline view by clicking "View Gridlines" on the Table Layout ribbon.

Appendix A. IRS Requirements for Safeguarding FTI

In addition to the MARS-E standards for Exchange systems, any system that receives, processes, or stores, and any devices that transmit, Federal Tax Information (FTI) must also comply with Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies* (available at www.irs.gov/uac/Safeguards-Program). Internal Revenue Code (IRC) section 6103 establishes FTI as confidential information with statutory protection under federal law, and provides criminal and civil sanctions for its unauthorized access or disclosure. All accesses and use of FTI must be monitored; FTI must always be identifiable and segregated from non-tax information to the maximum extent. The following paragraphs identify additional systemic controls that must be met.

Under the Affordable Care Act (ACA), the Centers for Medicare & Medical Services (CMS) Federal Data Services Hub (FDSH) may release, only with IRS approval, FTI through three (3) DSH services: H09, H15, H79 to Verify Annual Household Income and Family Size, evidenced by a Safeguard Security Report (SSR) approval letter. FTI may be disclosed to Marketplaces and state agencies administering Medicaid/Children's Health Insurance Program (CHIP) programs only as authorized by IRC 6103(l)(21), for use in making eligibility determinations for insurance affordability programs under provisions of the ACA. In order for agencies to receive IRS approval to obtain FTI, organizations must develop security policies and procedures that specifically protect FTI from unauthorized disclosure. The principles of need-to-know and least privilege should be incorporated when agencies grant systems and personnel access to FTI. Since CMS and IRS both developed their security standards based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, agencies are generally in compliance with the IRS standards when they meet the CMS-published MARS-E security requirements; however, there are some additional IRS requirements specified in Publication 1075 that are more stringent. Any agency facilities, information systems, and personnel that receive, process, transmit, or store FTI must also demonstrate the implementation of these additional IRS security requirements outlined in Table A-1. Administering entities submit IRS safeguard reports and requests for assistance concerning FTI directly to the IRS at Safeguardreports@irs.gov.

IRC Section 6103(p)(4)(E) requires agencies requesting FTI to report on the procedures established and used for ensuring the confidentiality of FTI. The IRS Office of Safeguards has the authority to conduct oversight and monitor the safeguarding measures employed through agency's annual submission of a SSR, semi-annual submission of an IRS Corrective Action Plan (CAP) to address any findings from an onsite review, and reporting certain changes with forty-five (45)-day notification to IRS, including when hiring a new contractor or subcontractor with access to FTI. See Publication 1075, Section 7 for more details. The Office of Safeguards will conduct periodic onsite reviews to evaluate the agency's use of FTI and the measures employed to protect the data. All agency and contractor facilities where FTI is received, processed, transmitted, or stored are subject to IRS review. Since information systems with FTI are often subsets of overarching systems managed by a Marketplace or state agency, the Office of Safeguards' review focuses on the compliance status of these system components only. Administering entities submit IRS safeguard reports and requests for assistance concerning FTI directly to the IRS at Safeguardreports@irs.gov.

Table A-1. Additional IRS Requirements for Safeguarding FTI

Control	CMS MARS-E	Additional IRS Publication 1075
Access Controls (AC)		
AC-2	• Authorizing access to the information system based on: a valid access authorization; intended system usage; and other attributes as required by the organization or associated missions/business functions.	• Authorize access to information systems that receive, process, store, or transmit FTI based on a valid access authorization, need-to-know permission, and under the authority to re-disclosed FTI under the provisions of IRC §6103 **See Publication 1075 Section 9.3.1.2 for details**
AC-3	• The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in information systems. Also see AC-2 (7): Role-based schemes for privileged user accounts	• The information system must enforce a role-based access control policy over defined subjects and objects and controls access to FTI based upon a valid access authorization, intended system usage, and the authority to be disclosed FTI under the provisions of IRC §6103. **See Publication 1075 Section 9.3.1.3 for details**
AC-7	• Configure the information system to lock out the user account automatically after three (3) invalid login attempts during a fifteen (15) minute time period. Require the lock out to persist for a minimum of (30) minutes.	• Enforce a limit of three (3) consecutive invalid logon attempts by a user during a 120-minute period; and automatically lock the account until released by an administrator. **See Publication 1075 Section 9.3.1.7 for details**
AC-17	The organization: • Documents allowed methods of remote access to the information system; • Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; • Authorizes remote access to the information system prior to allowing such connections; and • Monitors for unauthorized remote access to the information system	• Any remote access where FTI is accessed over the remote connection must be performed using multi-factor authentication. • FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore. **See Publication 1075 Section 9.3.1.12 for details**
AC-18	• Monitors for unauthorized wireless access to information systems by employing a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	• Selected CE-14 – Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. **See Publication 1075 Section 9.3.1.12 and Section 9.4.18, Wireless Networks for details**

Control	CMS MARS-E	Additional IRS Publication 1075
AC-20	• For *organizational users* (staff and contractors within the organization), 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, such as Personally Identifiable Information (PII), unless explicitly authorized, in writing, by the CIO or designated representative. If authorized, the organization establishes strict terms and conditions for their use. • For *non-organizational users* (such as business partners), the Administering Entity organization establishes terms and conditions, consistent with CMS implementation guidance of HHS Regulation 45 CFR §115.260, and in compliance with legal data sharing agreements signed with CMS, for any trust relationships established with other organizations owning, operating, and/or maintaining external information systems. These terms and conditions allow authorized individuals to: – Access the information system from external information systems; and – Process, store, or transmit organization-controlled information using external information systems.	• Unless approved by the Office of Safeguards, the agency must prohibit: a. Access to FTI from external information systems; b. Use of agency-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems; and c. (CE2) Use of non-agency-owned information systems; system components; or devices to process, store, or transmit FTI. • Any non-agency-owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation (see Section 7.4, 45-Day Notification Reporting Requirements). (CE3) **See Publication 1075 Section 9.3.1.15 for details**
AC-21	• Facilitates information sharing as defined in 45 CFR §155.260 (e), Privacy and Security of Personally Identifiable Information, 'Data 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 (as defined in data sharing agreements such as the Computer Matching Agreement or Information Exchange Agreement) where user discretion is required.	• The agency must restrict the sharing/re-disclosure of FTI on a need-to-know basis to only authorized individuals and uses of FTI specified by IRC §6103 and as approved by the Office of Safeguards. **See Publication 1075 Section 9.3.1.16 for details**
Audit and Accountability (AU)		
AU-2	• List of auditable events: Generate audit records for the following events: 1. List of auditable events: Generate audit records for the following events: a. Server alerts and error messages b. Log onto system. c. Log off system; d. Change of password;	• Specific implementation standards for audit events • Log onto system; • Log off of system; • Change of password; • All system administrator commands, while logged on as system administrator;

Control	CMS MARS-E	Additional IRS Publication 1075
	e. All system administrator commands, while logged on as system administrator; f. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS); g. Creation or modification of super-user groups; h. Subset of security administrator commands, while logged on in the security administrator role; i. Subset of system administrator commands, while logged on in the user role; j. Clearing of the audit log file; k. Startup and shutdown of audit functions; l. Use of identification and authentication mechanisms (e.g., user ID and password); m. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su); n. Remote access outside of the corporate network communication channels(e.g. modems, dedicated VPN) and all dial-in access to the system; o. Changes made to an applications or database by a batch file; p. Application-critical record changes; q. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility) r. User log-on and log-off (successful or unsuccessful) s. System shutdown and reboot; t. System errors; u. Application shutdown; v. Application restart; w. Application errors; and x. Security policy modifications; y. Printing sensitive information. 2. Subset of Implementation Standard 1 Enable logging for perimeter devices, including firewalls and routers: a. User log-on and log-off (successful or unsuccessful) b. Log packet screening denials originating from un-trusted networks, c. All system administration activities; d. Packet screening denials originating from trusted networks; e. Account creation, modification, or deletion of packet filters; f. System shutdown and reboot; g. System errors;	• Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS); • Creation or modification of super-user groups; • Subset of security administrator commands, while logged on in the security administrator role; • Subset of system administrator commands, while logged on in the user role; • Clearing of the audit log file; • Startup and shutdown of audit functions; • Use of identification and authentication mechanisms (e.g., user ID and password); • Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su); • Remote access outside of the corporate network communication channels(e.g., modems, dedicated VPN) and all dial-in access to the system; • Changes made to an application or database by a batch file; • Application-critical record changes; • Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility); • All system and data interactions concerning FTI; and • Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website. • Access to FTI must be audited at the operating system, software, and database levels. Software and platforms have differing audit capabilities. Each individual platform audit capabilities and requirements are maintained on the platform-specific Office of Safeguards SCSEM, which is available on the IRS Office of Safeguards website. **See Publication 1075 Section 9.3.3.3 for details**

Control	CMS MARS-E	Additional IRS Publication 1075
	h. Modification of proxy services. 3. Verify that proper logging is enabled in order to audit administrator activities.	
AU-4	• No documented requirement to ensure the allocation of audit storage capacity to retain audit records for the required retention time period.	• The agency must allocate audit record storage capacity to retain audit records for the required audit retention period of seven years. **See Publication 1075 Section 9.3.3.5 for details**
AU-6	• Specific implementation standards for audit log review processes include the following: – Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.	• If potential unauthorized FTI disclosure, report to TIGTA and IRS **See Publication 1075 Section 9.3.3.7 for details**
Security Assessment and Authorization (CA)		
CA-3	• Review and update the Interconnection Security Agreements on an ongoing basis.	• Review and update the system interconnection on an annual basis. **See Publication 1075 Section 9.3.4.3 for details**
Configuration Management (CM)		
CM-10	• Establishes restrictions on the use of open source software. Open source software must be legally licensed, approved by the agency information technology department, and adhere to a secure configuration baseline checklist from the US Government or industry.	• Selected CE1 – The agency must establish restrictions on the use of open source software. Open source software must: a. Be legally licensed; b. Be approved by the agency IT department; and c. Adhere to a secure configuration baseline checklist from the U.S. Government or industry. **See Publication 1075 Section 9.3.5.10 for details**
Contingency Planning (CP)		
CP-3	• Provide contingency training within 90 days of assuming role or responsibility.	• Provide contingency training prior to assuming role. **See Publication 1075 Section 9.3.6.3 for details**
Identification and Authentication (IA)		
IA-4	• 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 at least three (3) years has expired. • Disabling the identifier after sixty (60) days or less of inactivity and deleting disabled accounts during the annual re-certification process.	• Preventing reuse of identifiers • Disabling the identifier after 120 days **See Publication 1075 Section 9.3.7.4 for details**
IA-5	• Enforces at least four (4) changed characters or as determined by the information system (where possible) when new passwords are created; • Encrypts passwords in storage and in transmission; • Enforces password minimum and maximum lifetime restrictions of one (1) day minimum,	• Enforce privileged account passwords to be changed at least every 60 days; • Allow the use of a temporary password for system logons requiring an immediate change to a permanent password; and • Password-protect system initialization (boot) settings.

Control	CMS MARS-E	Additional IRS Publication 1075
	sixty (60) days maximum for user accounts, and 180 days for process-type accounts.	**See Publication 1075 Section 9.3.7.5 for details**
Incident Response (IR)		
IR-2	• Provide incident response training within 90 days of assuming role.	• Provide incident response training prior to assuming role. **See Publication 1075 Section 9.3.8.2 for details**
IR-6	• Require personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current Administering Entity (AE) organization Incident Handling Procedure and ACA incident handling process. • Report suspected incidents to the organizational incident response capability.	• Contact the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than 24 hours after identification of a possible issue involving FTI. • Section 10.0, *Reporting Improper Inspections or Disclosures*, for more information on incident reporting requirements required by the Office of Safeguards. **See Publication 1075 Section 9.3.8.6 for details**
Media Protection (MP)		
MP-3	• Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	• The agency must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating "Federal Tax Information". Notice 129-A and Notice 129-B IRS provided labels can be used for this purpose. **See Publication 1075 Section 9.3.10.3 for details**
MP-4	• Physically control and securely store magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks within organization-defined controlled area using a FIPS 140-2 validated encryption modules for digital media, and secure storage in locked cabinets or safes for non-digital media.	• Physically control and securely store media containing FTI. **See Publication 1075 Section 9.3.10.4 and Section 4.0 Secure Storage – IRC 6103(p)(4)(B) on additional secure storage requirements**
MP-6	• Sanitize digital and non-digital information system media in accordance with applicable federal and organizational standards and policies.	• Sanitize media containing FTI using IRS-approved sanitization techniques. **See Publication 1075 Section 9.3.10.6 for details. Additional requirements for protecting FTI during media sanitization are provided in Section 9.4.7, Media Sanitization, and Exhibit 10, Data Warehouse Security Requirements.**

Control	CMS MARS-E	Additional IRS Publication 1075
Physical and Environmental Protection (PE)		
PE-2	• 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 publically accessible). • Authorizes physical access to the facility where the information system resides and information is received, processed, stored, or transmitted based on position or role.	• Selected PE-1 – Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where FTI is received, processed, stored, or transmitted. **See Publication 1075 Section 9.3.11.2 for details**
PE-17	• Employ appropriate security controls at alternate work sites that include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate work sites; assesses as feasible, the effectiveness of security controls at alternate work sites; and provides a means for employees to communicate with information security personnel in case of security incidents or problems.	• Employ Office of Safeguards requirements at alternate work sites where FTI exists. Alternate work sites may include, for example, government facilities or private residences of employees (see Publication 1075 Section 4.7, Telework Locations, for additional requirements). **See Publication 1075 Section 9.3.11.9 for details**
Planning (PL)		
PL-2	• Develops a security plan for the information system that defines the authorization boundary for the system, describes the operational context of the system in terms of missions and business processes, describes the operational environment and relationships with or connections to other systems, provides an overview of the security requirements of the system and describes security controls in place or planned. Also ensure the plan is reviewed and approved by the authorizing official or designated representative prior to plan implementation.	• Implement this security control by developing an IRS Safeguard Security Report, to include the data flow specific to FTI, and submitting it to designated agency officials and submission of the signed report to the Office of Safeguards. **See Publication 1075 Section 9.3.12.2 for details**
Personnel Security (PS)		
PS-4	• Notify defined personnel or roles within one (1) business day.	• Notify agency personnel upon termination of the employee. **See Publication 1075 Section 9.3.13.4 for details**
PS-6	• Re-acknowledge access agreements when access agreements have been updated.	• Re-sign access agreements when access agreements have been updated or at least annually. **See Publication 1075 Section 9.3.13.6 for details**

Control	CMS MARS-E	Additional IRS Publication 1075
System and Service Acquisition (SA)		
SA-5	• Obtain administrator documentation that describes security configuration, installation, and operation of the system, use and maintenance of security functions and/or mechanisms, known vulnerabilities regarding configuration and use of administrative functions, methods for user interaction which enables individuals to use the system and user responsibilities in maintaining the security of the system.	• The agency must: – Protect documentation, as required; and – Distribute documentation to designated agency officials. **See Publication 1075 Section 9.3.15.5 for details**
SA-9	• Ensure service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.	• Agencies must prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit FTI unless explicitly approved by the Office of Safeguards. For notification requirements, refer to Section 7.4.5, Non-Agency-Owned Information Systems. • The contract for the acquisition must contain Exhibit 7 language, as appropriate (see Section 9.3.15.4, Acquisition Process (SA-4), and Exhibit 7, Safeguarding Contract Language). • FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore. Restrict the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations. **See Publication 1075 Section 9.3.15.7 for details**
System and Communications Protection (SC)		
SC-7	• Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system, implements sub networks for publicly accessible system components that are logically separated from internal organizational networks and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	• Additional requirements for protecting FTI on networks are provided in Publication 1075 Section 9.4.10, *Network Protections*. **See Publication 1075 Section 9.3.16.5 for details**

Control	CMS MARS-E	Additional IRS Publication 1075
SC-8	• Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by defined alternative physical safeguards. Cryptographic mechanisms implemented include cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical safeguards include protected distribution systems. • Maintains the confidentiality and integrity of information during preparation for transmission and during reception. • Install Intrusion Detection System (IDS) devices at network perimeter points and host-based IDS sensors on critical servers (SI-4).	• Implement cryptographic mechanisms to prevent unauthorized disclosure of FTI and detect changes to information during transmission across the wide area network (WAN) and within the local area network (LAN). • If encryption is not used, to reduce the risk of unauthorized access to FTI, the agency must use physical means (e.g., by employing protected physical distribution systems) to ensure that FTI is not accessible to unauthorized users. The agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic. **See Publication 1075 Section 9.3.16.6 for details**
SC-28	• The information system protects the confidentiality and integrity of information at rest. This control covers user as well as system information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections including the use of cryptographic mechanisms and file share scanning. • When cryptographic mechanisms are used, the information system implements encryption products that have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, directives, policies, regulations, and standards. (SC-13).	• The confidentiality and integrity of information at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms. • FTI stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology. • Mobile devices do require encryption at rest (see Publication 1075 Section 9.3.1.14, Access Control for Mobile Devices (AC-19), and Section 9.4.8, Mobile Devices. **See Publication 1075 Section 9.3.16.15 for details**
System and Information Integrity (SI)		
SI-2	• Installs security-relevant software and firmware updates on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days.	• Install security-relevant software and firmware updates based on severity and associated risk to the confidentiality of FTI. **See Publication 1075 Section 9.3.17.2 for details**

Control	CMS MARS-E	Additional IRS Publication 1075
SI-4	• Monitors the information system to detect attacks and indicators of potential attacks, unauthorized local, network, and remote connections. • Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.	• Selected CE4 – Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. • Selected CE7 – Notify designated agency officials of detected suspicious events and take necessary actions to address suspicious events • Selected CE11 – Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications. • Selected CE23 – Implement host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit FTI. **See Publication 1075 Section 9.3.17.4 for details**
Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques (Enhancement) (DM-3 (1)) –PRIVACY CONTROL		
DM-3 (1)	• The Organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training. • Organizations can minimize risk to privacy of PII using techniques such as de-identification or randomly generate data to match PII characteristics.	• FTI may never be de-identified or randomized. FTI includes any information created by the recipient that is derived from return or return information. FTI may not be masked to change the character of information to circumvent requirements under IRC 6103.
Cloud Computing Environments		
N/A		• Notification Requirement • Data Isolation • SLA • Data Encryption in Transit • Data Encryption at Rest • Persistence of Data in Relieved Assets • Risk Assessment • Security Control Implementation **See Publication 1075 Section 9.4.1 for details**
Data Warehouse		
N/A		**See Publication 1075 Section 5.2, Section 9.4.2, and Exhibit 10, Data Warehouse Security Requirements, for details.**
Email Communications		
N/A		• If FTI is prohibited from inclusion within emails or email attachments, a policy must be written and distributed. • If FTI is allowed to be included within emails or email attachments, the agency must only transmit FTI to an authorized recipient and must adhere to Publication 1075 requirements. **See Publication 1075 Section 9.4.3 for details**

Control	CMS MARS-E	Additional IRS Publication 1075
Fax Equipment		
N/A		• If FTI is prohibited from inclusion within fax communications, a policy must be written and distributed. • If FTI is allowed to be included within fax communications, the agency must only transmit FTI to an authorized recipient and must adhere to Publication 1075 requirements. **See Publication 1075 Section 9.4.4 for details**
Integrated Voice Response (IVR) Systems		
N/A		• To use an IVR system that provides FTI over the telephone to a customer, the agency must meet the Publication 1075 requirements. **See Publication 1075 Section 9.4.5 for details**
Live Data Testing		
N/A		• The use of live FTI in test environments should generally be avoided and is not authorized unless specifically approved by the Office of Safeguards through the submission of a Data Testing Request (DTR) form. **See Publication 1075 Section 9.4.6 for details**
Multi-Functional Devices (MFD)		
N/A		• To use FTI in a multi-functional device, the agency must meet the Publication 1075 requirements. **See Publication 1075 Section 9.4.9 for details**
Storage Area Networks (SAN)		
N/A		• To use FTI in a SAN environment, the agency must meet the Publication 1075 requirements. **See Publication 1075 Section 9.4.11 for details**
System Component Inventory		
N/A		• The agency must maintain a current inventory of information systems that receive, process, store, or transmit FTI in both production and pre-production environments. Updates to the inventory should be a critical step when implementing installations, removals, and updates to the information system. The inventory should accurately reflect and be consistent with the security domain of the current information system to enable the detection of unauthorized access to FTI within production and pre-production environments. **See Publication 1075 Section 9.4.12 for details**

Control	CMS MARS-E	Additional IRS Publication 1075
Virtual Desktop Infrastructure (VDI)		
N/A		• To use VDI that provides FTI to a customer, the agency must meet the Publication 1075 requirements. **See Publication 1075 Section 9.4.13 for details**
Virtualization Environments		
N/A		• To use a virtual environment that receives, processes, stores, or transmits FTI, the agency must meet the Publication 1075 requirements. **See Publication 1075 Section 9.4.14 for details**
VoIP Systems		
N/A		• To use a VoIP network that provides FTI to a customer, the agency must meet the Publication 1075 requirements. **See Publication 1075 Section 9.4.15 for details**
Web-Based Systems		
N/A		• To use an external web-based system or website that provides FTI over the Internet to a customer, the agency must meet the Publication 1075 requirements. **See Publication 1075 Section 9.4.16 for details**
Web Browser		
N/A		• To access FTI using a web browser, the agency must meet the Publication 1075 requirements. **See Publication 1075 Section 9.4.17 for details**

Appendix B. Security and Privacy Agreements and Compliance Artifacts

ACA Administering Entities (AE) and their business partners are required to manage their information system(s) using an organization defined system development life cycle (SDLC) that integrates security into the development, implementation, and operation of the information system and continues through maintenance and disposal. Table B-1 provides a list of required security and privacy agreements and compliance artifacts for AE systems to implement throughout the information system life cycle process to include Artifacts and Agreements required for requesting an authority to connect and/or prior to production and during the maintenance of systems in the production stage.

Table B-1. MARS-E Security and Privacy Agreements and Compliance Artifacts

Artifact Title	Security Control Reference	Privacy Control Reference	Required for ATC	Reference as part of the SSP[1]	Required to be delivered to CMS	Artifact Submission Timelines	Guidance/ Template Available on CALT	AE Supply Plan to Submit Date
ARTIFACTS REQUIRED BEFORE SYSTEM ENTERS THE PRODUCTION STAGE AND BEFORE ATC								
Privacy Impact Assessment (PIA)		AR-2	X		X	90 days before system enters production stage; 90 days before ATC	X	
Computer Matching Agreement (CMA)		AP-1	X		X	60 days before system enters production stage; 60 days before ATC	X	
Information Exchange Agreement (IEA)		AP-1	X		X	60 days before system enters production stage; 60 days before ATC	X	
Fed2NonFed Interconnection Security Agreement (ISA)	CA-3 CA-6		X		X	60 days before system enters production stage; 60 days before ATC	X	
Plan of Action and Milestones (POAMs)	CA-5		X		X	30 days before system enters production stage; 30 days prior to ATC	X	

[1] These artifacts must be referenced in the SSP by title and date, but are not necessarily required to be delivered to CMS or uploaded to CALT; the Independent Assessor will review and verify.

Artifact Title	Security Control Reference	Privacy Control Reference	Required for ATC	Reference as part of the SSP[1]	Required to be delivered to CMS	Artifact Submission Timelines	Guidance/ Template Available on CALT	AE Supply Plan to Submit Date
Final System Security Plan (SSP) • Part A – System Identification • Part B – Security Controls Workbook • Part C – Privacy Controls Workbook • Part D – SSP Attachments	PL-2		X		X	60 days before system enters production stage; 60 days prior to ATC and reviewed / updated annually	X	
Required SSP Attachments • Detailed Configuration Settings • Software and Hardware Inventory • Information Security Risk Assessment (ISRA)	PL-2 CM-6 CM-8		X	X	X	60 days before system enters production stage 60 days prior to ATC and reviewed / updated annually	X	
IRS Safeguard Security Report (SSR) Approval Letter			X[2]	X IRS required security controls must be documented in SSP	Do not submit IRS reports to CMS	Contact IRS to coordinate SSR submission as soon as the need for FTI is identified	SSR template available at: http://www.irs.gov/uac/Safeguards-Program	

[2] The Exchange Blueprint requires an IRS approval letter to receive Federal tax information (FTI) from the Annual Income and Family Size Verification Hub service for an Individual Marketplace. AEs requesting FTI for Medicaid/CHIP eligibility determinations also require an IRS-approved SSR and above CMS baseline configuration for systems processing FTI – contact IRS at: Safeguardreports@irs.gov.

Artifact Title	Security Control Reference	Privacy Control Reference	Required for ATC	Reference as part of the SSP[1]	Required to be delivered to CMS	Artifact Submission Timelines	Guidance/ Template Available on CALT	AE Supply Plan to Submit Date
Independent (3rd Party) Assessor Security Test Plan and Test Results Report (SAR)	CA-2 CA-2 (1)		X	X	X	60 days before system enters production stage; 60 days prior to ATC (then every 3 years)	X	
Contingency Plan and Test Plan[3]	CP-2			X		60 days before system enters production stage; 60 days prior to ATC as part of SSP, and reviewed annually		
Contingency Plan Test Results[4]	CP-4			X		60 days before system enters production stage; 60 days prior to ATC as part of SSP, and reviewed annually		
Incident Response Plan (IRP)[5]	IR-8			X		60 days before system enters production stage; 60 days prior to ATC as part of SSP, and reviewed annually	X	

3 Artifacts are part of Independent Assessor review

4 Artifacts are part of Independent Assessor review.

5 Artifacts are part of Independent Assessor review.

Artifact Title	Security Control Reference	Privacy Control Reference	Required for ATC	Reference as part of the SSP[1]	Required to be delivered to CMS	Artifact Submission Timelines	Guidance/ Template Available on CALT	AE Supply Plan to Submit Date
Training Plan[6]	AT-1			X		60 days before system enters production stage; 60 days prior to ATC as part of SSP, and reviewed annually		
Intrastate/Interstate MOU/ISA[7]	CA-3			X		60 days before system enters production stage; 60 days prior to ATC as part of SSP, and reviewed annually		
Configuration Management Plan[8] F	CM-9			X		60 days before system enters production stage; 60 days prior to ATC as part of SSP, and reviewed annually		
Information Security Risk Assessment (ISRA)[9]	RA-3			X	X	60 days before system enters production stage; 60 days prior to ATC as part of SSP, and reviewed annually	X	

6 Artifact is part of Independent Assessor review.

7 Artifact is part of Independent Assessor review.

8 Artifact is part of Independent Assessor review.

9 Artifact is required during the systems life cycle development process, part of Independent Assessor review, and should be delivered to CMS as an attachment to the SSP.

Artifact Title	Security Control Reference	Privacy Control Reference	Required for ATC	Reference as part of the SSP[1]	Required to be delivered to CMS	Artifact Submission Timelines	Guidance/ Template Available on CALT	AE Supply Plan to Submit Date
REQUIREMENTS FOR ANNUAL REPORTING (Maintenance of AE Systems in the Production Stage)								
Privacy Impact Assessment (PIA) Update		AR-2		X		Annually or when changes to the privacy program occurs	X	
Final System Security Plan (SSP) • Part A – System Identification • Part B – Security Controls Workbook • Part C – Privacy Controls Workbook • Part D – SSP Attachments				X		Annually	X	
Required SSP Attachments • Detailed Configuration Settings • Software and Hardware Inventory • Information Security Risk Assessment (ISRA)				X		Annually	X	

Artifact Title	Security Control Reference	Privacy Control Reference	Required for ATC	Reference as part of the SSP[1]	Required to be delivered to CMS	Artifact Submission Timelines	Guidance/ Template Available on CALT	AE Supply Plan to Submit Date
Annual Security Attestation (**Compliance Report**) based on reviews of SSP including the ISRA, Contingency Plan, Training Plan, ISA, CMA, and IEA	CA-2 CA-7 CA-7 (1)		X[10]		X	Annually	X	
Independent (3rd Party) Assessor Security Test Plan and Test Results Report (SAR)[11] **Optional Deliverable for Annual Attestation**	CA-2 CA-7 CA-7 (1)				X	Annually	X	
IRS Safeguard Security Report						Annually See Pub 1075 Sec 7.2 for state schedule		
QUARTERLY REPORTING								
POAMs	CA-5 PM-4				X	January 31 April 30 July 31 October 31		

[10] May be required if using three (3) independent assessments for annual attestations and using those for ATC renewal. If this is done each of the three (3) years between full ATCs by an independent assessor, they can then use these assessments for the renewal.

[11] The SAR is an optional deliverable for the annual reviews; organizations may choose to use an Independent Assessor.

Artifact Title	Security Control Reference	Privacy Control Reference	Required for ATC	Reference as part of the SSP[1]	Required to be delivered to CMS	Artifact Submission Timelines	Guidance/ Template Available on CALT	AE Supply Plan to Submit Date
REQUIREMENTS FOR CHANGE REPORTING[12]								
AE System Change/Security and Privacy Impact Analysis Notification (CN) Form	CM-3, CM-4				X	60 days prior to plan implementation	X	

[12] Based on the specific change type, the states may be required to produce additional or updated artifacts or obtain new ATC; see Change Reporting Procedures referenced.

Master List of Acronyms for MARS-E Document Suite

AC	Access Control, a Security Control family
ACA	Patient Protection and Affordable Care Act of 2010
AE	Administering Entity
AP	Authority and Purpose, a Privacy Control family
API	Application Programming Interface
APT	Advanced Persistent Threat
AR	Accountability, Audit, and Risk Management, a Privacy Control family
AT	Awareness and Training, a Security Control family
ATC	Authority to Connect
ATO	Authorization to Operate
AU	Audit and Accountability, a Security Control family
BHP	Basic Health Program
BIOS	Basic Input Output System
BPA	Blanket Purchase Agreement
CA	Security Assessment and Authorization, a Security Control family
CAG	Consensus Audit Guidelines
CAP	Corrective Action Plan
CCIIO	Center for Consumer Information and Insurance Oversight
CE	Control Enhancement
CFR	Code of Federal Regulation
chown	Change Owner
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management, a Security Control family
CMA	Computer Matching Agreement
CMPPA	Computer Matching and Privacy Protection Act of 1988
CMS	Centers for Medicare & Medicaid Services
COTS	Commercial Off-the-Shelf
CP	Contingency Planning, a Security Control family

CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DI	Data Quality and Integrity, a Privacy Control family
DISA	Defense Information Systems Agency
DM	Data Minimization and Retention, a Privacy Control family
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	DNS Security
DoD	Department of Defense
DR	Disaster Recovery, a Security Control family
DSH	CMS Data Services Hub
DTR	Data Testing Report
EAP	Extensible Authentication Protocol
EHR	Electronic Healthcare Record
FDSH	Federal Data Services Hub
FFM	Federally-facilitated Marketplace
FIPPS	Fair Information Protection Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTI	Federal Tax Information
FTP	File Transfer Protocol
GAGAS	Generally Accepted Governmental Auditing Standards
GMT	Greenwich Meridian Time
guid	Globally Unique Identifier
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996

HITECH	Health Information Technology for Economic and Clinical Health Act of 2009
HTTP	Hypertext Transfer Protocol
IA	Identification and Authentication, a Privacy Control family
ID	Identity
IDS	Intrusion Detection System
IEA	Information Exchange Agreement
IIHI	Individually Identifiable Health Information
IP	Internet Protocol
IP	Individual Participation and Redress, a Privacy Control family
IPS	Intrusion Prevention System
IR	Incident Response, a Privacy Control family
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS	Information Security
IS	Information System
ISA	Information Sharing Agreement
ISE	Information Sharing Environment
ISPG	Information Security Privacy Policy and Compliance Group
ISRA	Information Security Risk Assessment
IT	Information Technology
MA	Maintenance, a Security Control family
MAC	Media Access Control
MAGI	Modified Adjusted Gross Income
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MFD	Multi-Function Device
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

NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
NVD	National Vulnerability Database
OEI	Office of Enterprise Information
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OVAL	Open Vulnerability Assessment Language
PDA	Portable Digital Assistant
PDF	Portable Document Format
PE	Physical and Environmental Protection, a Security Control family
PEAP	Protected Extensible Authentication Protocol
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
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
QHP	Qualified Health Plan
RA	Risk Assessment, a Security Control family
RTO	Recovery Time Objectives
RUNAS	Microsoft command (allowing user to run specific tools and programs with different permissions other than as provided by user's current logon)
SA	System and Services Acquisition, a Security Control family
SAN	Storage Area Network
SAOP	Senior Agency Office for Privacy
SBM	State-based Marketplace
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
sftp	Secured File Transfer Protocol
SI	System and Information Integrity, a Security Control family
SIA	Security Impact Analysis
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMART	SBM Annual Reporting Tool
SNA	Systems Network Architecture (IBM)
SORN	System of Record Notice
SOW	Statement of Work
SP	Special Publication
SSA	Social Security Administration
SSH	Secure Shell
SSP	System Security Plan
SSR	Safeguard Security Report
su	Substitute User Change user ID or become superuser
suid	Set User ID
TCP	Transmission Control Protocol
TIGTA	Treasury Inspector General for Tax Administration
TLS	Transport Layer Security
TR	Transparency, a Privacy Control family
UHF	Ultra High Frequency
UL	Use Limitation, a Privacy Control family
URL	Universal Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Response Team
USGCB	United States Government Configuration Baseline
UTC	Universal Time Coordinate
UUENCODE	Unix-to-Unix Encode
VA	Department of Veterans Affairs

VDI	Virtual Desktop Infrastructure
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WIDS/WIPS	Wireless Intrusion Detection/Prevention System
WORM	Write-Once-Read-Many

Master Glossary for MARS-E Document Suite

Administering Entity (AE)	Exchanges, whether federal or state, state Medicaid agencies, state Children's Health Insurance Program (CHIP) agencies, or state agencies administering the Basic Health Program (BHP), or an entity established under Section 1311 of the ACA.
Affordable Care Act (ACA)	The comprehensive health care reform law enacted in March 2010. The law was enacted in two parts: The Patient Protection and Affordable Care Act was signed into law on March 23, 2010 and was amended by the Health Care and Education Reconciliation Act on March 30, 2010. The name "Affordable Care Act" is used to refer to the final, amended version of the law. The law's official title is the Patient Protection and Affordable Care Act of 2010 (Public Law No. 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law No. 111-152) (collectively, the ACA).
Authority to Connect (ATC)	This term is used in the execution of the Interconnection Security Agreement (ISA) with CMS. An "Authority to Connect (ATC)" by CMS is required to activate a system-to-system connection to the Data Services Hub.
Basic Health Program (BHP)	An optional state basic health program established under Section 1331 of the ACA. The Basic Health Program provides states with the option to establish a health benefits coverage program for lower-income individuals as an alternative to Health Insurance Marketplace coverage under the Affordable Care Act. This voluntary program enables states to create a health benefits program for residents with incomes that are too high to qualify for Medicaid through Medicaid expansion in the Affordable Care Act, but are in the lower income bracket to be eligible to purchase coverage through the Marketplace.
Breach	Defined by Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control, or any similar term or phrase that refers to situations where persons other than authorized users or for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Children's Health Insurance Program (CHIP)	CHIP is a state-run federal health insurance program for uninsured children up to age 19 in families with too much income to qualify for Medicaid (Medical assistance) and that cannot afford to purchase health insurance. The state program was established under Title XXI of the Social Security Act.
Computer Matching Agreement (CMA)	An agreement that an organization enters into in connection with a computer matching program to which the organization is a party. A CMA is required for any computerized comparison of two or more systems of records or a system of records of non-federal records for the purpose of (1) establishments or verifying eligibility or compliance with law and regulations of applicants or recipients/beneficiaries, or (2) recouping payments or overpayments. One purpose of such a program is to establish or verify the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs.
Digital Identity	The electronic representation of a real-world entity, and is usually taken to represent the online equivalent of a real individual. This online equivalent of an individual participates in electronic transactions on behalf of the individual it represents. Typically, digital identities are established and represented in the form of a unique identifier, such as a User ID, to represent an individual during a transaction.
Fair Information Practice Principles (FIPP)	Eight principles that provide the basis for these privacy controls, and are rooted in the federal Privacy Act of 1974, §208 of the E-Government Act of 2002, and Office of Management and Budget policies. The principles are transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing. The FIPPs are designed to build public trust in the privacy practices of organizations, and to help organizations avoid tangible costs and intangible damages from privacy incidents. The FIPPs are recognized in the U.S. and internationally as a general framework for privacy. Marketplace privacy and security regulations at 45 CFR §155.260(a) (3) (i)-(viii) require that Marketplaces establish and implement privacy and security standards that are consistent with and align with the eight principles of the FIPPs.
Federal Tax Information (FTI)	Defined broadly by the Internal Revenue Service (IRS) as including, but not limited to, any information, besides the return

	itself, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRS Code for any tax, penalty, interest, fine, forfeiture, or other imposition or offense; information extracted from a return, including names of dependents or the location of a business; the taxpayer's name, address, and identification number; information collected by the IRS about any person's tax affairs, even if identifiers are deleted; whether a return was filed, is or will be examined, or subject to other investigation or processing; and information collected on transcripts of accounts (for more information, see IRS Code §6103).
Federally-Facilitated Marketplace (FFM)	A Marketplace established and operated within a state by the Department of Health and Human Services (HHS) and operated by CMS under Section 1321(c) (1) of the ACA.
Federal Data Services Hub (Hub or FDSH)	The CMS federally managed service to transmit data between federal and state Administering Entities and to interface with federal agency partners and data sources.
Health Insurance Exchange (HIX)	A governmental agency or non-profit entity that meets the applicable standards of this part and makes Qualified Health Plans (QHP) available to qualified individuals and/or qualified employers. Unless otherwise identified, this term includes an Exchange serving the individual market for qualified individuals and a Small Business Health Options Program (SHOP) serving the small group market for qualified employers, regardless of whether the Exchange is established and operated by a state (including a regional Exchange or subsidiary Exchange) or by HHS.
Identity Proofing	In the context of the ACA, refers to a process through which the Marketplace, state Medicaid agency, or state CHIP agency obtains a level of assurance regarding an individual's identity that is sufficient to allow access to electronic systems that include sensitive (i.e., Personally Identifiable Information) state and federal data.
Incident	Means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. Incident means the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement

	of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction. While certain adverse events, (e.g., floods, fires, electrical outages, and excessive heat) can cause system crashes, they are not considered incidents. An Incident becomes a Breach when there is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access to personally identifiable information or personal health information, whether physical or electronic.
Information Exchange Agreement (IEA)	Agreement with CMS documenting the terms, conditions, safeguards, and procedures for exchanging information, when the information exchange is not covered by a computer matching agreement.
Information Security Risk Assessment (ISRA)	An analysis performed to assess the risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. The Information Security Risk Assessment process is used to provide the Business Owners with the means to continuously identify and mitigate business and system risks throughout the life cycle of the system.
Insurance Affordability Program	Program under Title I of the ACA for the enrollment in qualified health plans offered through a Marketplace, including but not limited to, enrollment with Advanced Premium Tax Credits (APTC) and Cost Sharing Reductions (CSR); (2) a State Medicaid program under Title XIX of the Social Security Act; (3) a state Children's Health Insurance Program (CHIP) under Title XXI of the Social Security Act; and (4) a state program under Section 1331 of the ACA establishing qualified basic health plans.
Interconnection Security Agreement (ISA)	Used for managing security risk exposures created by the interconnection of a system to another system owned by an external entity. Both parties agree to implement a set of common security controls. An "Authority to Connect (ATC)" by CMS is required to activate a system-to-system connection to the Data Services Hub.
IRS Safeguard Security Report (SSR)	Required by 26 U.S.C. §6103(p)(4)(E) and filed in accordance with IRS Publication 1075 to detail the safeguards established to

	maintain the confidentiality of Federal Tax Information (FTI) through the Hub or in an account transfer containing FTI.
Itemized Consent	See definition for Tiered Consent.
Layered Notice	A privacy notice approach that involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed and specific information.
Marketplace (or Exchange)	American Health Exchange established under Sections 1311(b), 1311(d), or 1321(c) (1) of the ACA, including both State-based Marketplaces (SBM) and Federally-Facilitated Marketplaces. The use of the term "Marketplace" in this Framework indicates that a control applies to both SBMs and FFMs.
Medicaid	The Medicaid program was established under Title XIX of the Social Security Act, together with other health care programs established under state law.
Multi-Factor Authentication (MFA)	Multi-factor authentication refers to the use of more than one of the following factors. The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication: • Something you know (for example, a password) • Something you have (for example, an ID badge or a cryptographic key) • Something you are (for example, a fingerprint or other biometric data) The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors.
Non-Exchange Entity (NEE or Non-Marketplace Entity)	Also referred to as a "non-Exchange entity" (NEE) and as defined in regulation at 45 CFR §155.260(b), as, "any individual or entity that: (i) Gains access to personally identifiable information submitted to a Marketplace; or (ii) Collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Marketplace. […]"

Personally Identifiable Information (PII)	As defined by National Institute of Standards and Technology (NIST) Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."
Privacy Act Statement (PAS)	A notice that provides the authority of the Marketplace or Administering Entity to collect PII; whether providing PII is mandatory or optional; the principal purpose(s) for which the PII is to be used; the intended disclosure (routine uses) of the PII; and the consequences of not providing all, or some portion of, the PII requested.
Privacy Impact Assessment (PIA)	The process and document that is the outcome of the process of identifying privacy risks and methods to mitigate them. PIAs are performed before developing or procuring information systems, or initiating programs or projects that collect, use, maintain, or share PII, and they are updated when changes create new privacy risks. PIAs also are conducted to ensure that programs and information systems comply with applicable legal, regulatory, and policy requirements.
Real-time Notice	A privacy notice provided to the individual at the point of collection of information.
Qualified Health Plan (QHP)	Under the Affordable Care Act, an insurance plan that is certified by the health insurance Marketplace, provides essential health benefits, follows established limits on cost sharing (like deductibles, copayments, and out-of-pocket maximum amounts), and satisfies other requirements. A QHP has a certification by each Marketplace in which it is sold.
Qualified Individual	With respect to a Marketplace, an individual who has been determined eligible to enroll through the Marketplace in a qualified health plan in the individual market.
Remote Identity Proofing (RIDP)	Refers to a commonly used process to instantly identity proof the claimed identity of an individual over the Internet, such as an unknown visitor to an Administering Entity web portal.

Security Impact Analysis (SIA)	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
State-Based Marketplace (SBM)	As authorized by the Affordable Care Act, a health insurance Marketplace established and operated within a state, for which the state determines the specific criteria for plan certification and participation within broad federal regulations, and maintains local authority over managing health plans in the Marketplace.
State-Based Privacy and Security Artifacts	These are state-based privacy and security agreements to govern relationships where data sharing or system connections occur at the state level. All agreements at the state-level must bind the other party to meeting the same or more stringent privacy and security requirements than what is specified within 45 C.F.R. §155.260 (security standards are enumerated within the MARS-E Suite of documents). The state is responsible for the form these agreements take, such as contracts, Service Level Agreements, or memoranda of understanding.
System of Records	Defined in the Privacy Act at 5 U.S.C. §552a(a) (5). It is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
System of Records Notice (SORN)	A statement that provides public notice of the existence and character of a group of records under the control of any agency, from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual (for more information, see OMB Circular A-130, *Federal Agency Responsibilities for Maintaining Records About Individuals*).
System Security Plan (SSP)	As defined by NIST Special Publication Special Publication 800-37, an SSP is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Tiered Consent	Also referred to as itemized consent, provides a means for individuals to authorize the collection, use, maintenance, and sharing of PII before its collection; provides a means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, or retention of PII; obtains individuals' consent to any new uses or disclosures of previously collected PII; and

ensures that individuals are aware of and consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.