CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-17 Medicare Business Partners Systems Security	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 14	**Date: June 15, 2018**
	Change Request 10576

SUBJECT: IOM 100-17 Updates

I. SUMMARY OF CHANGES: To address a continually changing CMS security environment, the CMS Medicare Contractor Management Group (MCMG) has updated IOM 100-17 which contains the Business Partner System Security Manual (BPPSM) and the Medicare Administrative Contractor (MAC) Acceptable Risk Safeguards (ARS). Changes to the BPSSM and MAC ARS were necessary as a result of the CMS Information Security and Privacy Group (ISPG) updating the CMS ARS from version 3.0 to version 3.1.

The purpose of this CR is to have the MACs perform an analysis regarding the attached BPSSM revision 14 including the updated MAC ARS security requirements to evaluate cost and operational impacts, and to provide a level of effort to CMS detailing what is required to implement the updates. In order to assist you with your evaluation, any changes from revision 13 to revision 14 of the BPSSM are highlighted in red. Additionally, an attachment has been included with this CR that contains information about controls that have changed from ARS 3.0 to ARS 3.1.

As part of this process for considering implementation of the updated security requirements, the MACs shall review the updated BPSSM and MAC ARS control set to evaluate the documented requirements to fully determine possible impacts. MACs shall consider the workload associated with the planning, implementation, education and ongoing support required to meet the security requirements in their analysis.

EFFECTIVE DATE: November 30, 2018
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: November 30, 2018

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	1/Introduction
R	1.1/Additional Requirements for MACs
R	2.2/Principal Systems Security Officer (SSO)
R	3.01/Control Components
R	3.02/Reporting Requirements
R	3.2/Risk Assessment (RA)
R	3.4/Certification
R	3.5.1/Annual FISMA Assessment (FA)
R	3.5.2/Plan of Action and Milestones
R	3.5.3/Timing Requirements for Compliance Conditions
R	3.6/Security Incident Reporting and Response
R	3.10/Patch Management
R	3.11/Security Configuration Management
R	3.11.1/Security Technical Implementation Guides (STIG)
R	3.11.3/National Institute of Standards and Technology (NIST)
R	3.12/End of Life Technology Components
R	3.13/Cloud Computing
N	3.14/MAC ARS Control Tailoring
N	3.15/Data Loss Prevention
N	3.16/Wireless Access Monitoring
N	3.17/Malicious Software
N	3.18/Whitelisting
N	3.19/Data Encryption
R	4.1.2/Security Level by Information Type
R	4.1.4/Minimum System Security Requirements—HIGH
R	5/Internet Security
R	Appendix A/1/Introduction
R	Appendix B/2/Safeguards against Employee Fraud
R	Attachment 1/MAC ARS

III. FUNDING:

For Medicare Administrative Contractors (MACs):

The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is

not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:

Business Requirements
Manual Instruction

Attachment - Business Requirements

Pub. 100-17	Transmittal: 14	Date: June 15, 2018	Change Request: 10576

SUBJECT: IOM 100-17 Updates

EFFECTIVE DATE: November 30, 2018
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: November 30, 2018

I. GENERAL INFORMATION

A. Background: This is an update to the existing Business Partners Systems Security Manual (BPSSM) and the Medicare Administrative Contractor (MAC) requirements regarding the CMS Acceptable Risk Safeguards (ARS). The BPSSM provides clarification and support to various CMS security policies, standards guidelines and procedures. The MAC Acceptable Risk Safeguards (ARS) are based on NIST Special Publication 800-53 Revision 4, dated April 2013 and have been customized for usage by the MACs.

B. Policy: This CR is to ensure compliance with the Federal Information Security Management Act (FISMA) of 2002, National Institute of Standards and Technology (NIST) requirements and guidance, and CMS policies, standards, guidelines and procedures.

II. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement, and "should" denotes an optional requirement.

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
10576.1	Contractors shall be in compliance with any requirements updated in the Business Partner System Security Manual (BPSSM) and Medicare Administrative Contractor (MAC) Acceptable Risk Safeguards (ARS).	X	X	X	X					
10576.2	Medicare Administrative Contractors (MACs) shall perform an analysis to determine level of effort to implement any updates to BPSSM version 14 and the associated MAC Acceptable Risk Safeguards (ARS). Relationships with any affected subcontractors should be considered/included in the analysis and the impacts to the subcontractor should be identifiable within the analysis.	X	X	X	X					
10576.2.1	For the MAC ARS, a document (Change List for New MAC ARS.docx) has been provided (in the Forum) that attempts to identify changes that could have an	X	X	X	X					

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	impact on implementing the updated MAC ARS controls as a result of the issuance of the CMS ARS 3.1. This document is provided as a guide only and may not be all inclusive.									
10576.2.2	MACs shall provide analysis and costs for the following MAC ARS controls that were not included in the earlier version. Specifically, MACs should evaluate and address AC-17(9), CA-9(1), MA-4(1), DI-1(2), DI-2, DI-2(1) and DM-1(1).	X	X	X	X					
10576.2.3	For this CR, MACs shall not consider or provide any workload estimates for part or all of any requirements that necessitate interaction/effort with the CMS Cybersecurity Integration Center (CCIC), even if they have changed from the prior version.	X	X	X	X					
10576.2.4	Upon completion of the analysis of the proposed BPSSM and MAC ARS changes, MACs shall provide an estimate that details the level of effort ***by each specified control*** for implementing any required changes. The MACs shall evaluate all changes and submit only those changes that will result in cost and effort changes within their environment. This estimate should be delivered to Frank Schreibman, (Frank.Schreibman@cms.hhs.gov) and uploaded to the CR estimates portion of ECHIMP. Any submission that does not clearly indicate the control, actions necessary and level of effort for a specific change will be returned for updating.	X	X	X	X					

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility				
		A/B MAC			DME MAC	CEDI
		A	B	HHH		
	None					

IV. SUPPORTING INFORMATION

Section A: Recommendations and supporting information associated with listed requirements: N/A

"Should" denotes a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: All other recommendations and supporting information: N/A

V. CONTACTS

Pre-Implementation Contact(s): Gregg Sanders, 410-786-1936 or Gregg.Sanders@cms.hhs.gov , Frank Schreibman, 410-786-0336 or Frank.Schreibman@cms.hhs.gov , Kevin Potter, 410-786-5686 or Kevin.Potter@cms.hhs.gov

Post-Implementation Contact(s): Contact your Contracting Officer's Representative (COR).

VI. FUNDING

Section A: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

ATTACHMENTS: 1

Centers for Medicare & Medicaid Services (CMS)

Business Partners

Systems Security Manual

CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

(Rev.14, Issued: 06-15-18)

CMS/ Business Partners
Systems Security Manual

Record of Changes

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Revision	Major Changes	Date
12	Main Document and all Appendices (1) Updated Internet hyperlinks throughout document (2) Changed "EISG" (Enterprise Information Security Group) to "ISPG" (Information Security and Privacy Group" throughout document (3) Correct typographical errors	08/2013
13	Main Document and all Appendices (1) Deleted Section 3.6.1/Computer Security Incident Response due to duplication (2) Added Section 3.12/End Of Life Technology Components (3) Added Section 3.13/Cloud Computing (4) Added Attachment 1/MAC ARS	06/2017
14	*Main Document and all Appendices* *(1) Updated ARS 3.x to MAC ARS where appropriate* *(2) Added Section 3.14/MAC ARS Control Tailoring* *(3) Added Section 3.15/Data Loss Prevention* *(4) Added Section 3.16/Wireless Access Monitoring* *(5) Added Section 3.17/Malicious Software* *(6) Added Section 3.18/Whitelisting* *(7) Updated outdated content as appropriate.*	04/2018

CMS/Business Partners
Systems Security Manual

Table of Contents

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Table of Contents

1 - Introduction
- 1.1 - Additional Requirements for MACs

2 - IT Systems Security Roles and Responsibilities
- 2.1 - CMS Contracting Officer's Representative (COR)
- 2.2 - Principal Systems Security Officer (SSO)
- 2.3 – CMS Business Owners
- 2.4 – CMS System Maintainers/Developers
- 2.5 - Personnel Security/Suitability

3 - IT Systems Security Program Management
- 3.01 - Control Components
- 3.02 - Reporting Requirements
- 3.1 - System Security Plan (SSP)
- 3.2 - Risk Assessment (RA)
- 3.3 - Contingency Planning
- *3.4* - Certification
- 3.5 - Compliance
- 3.5.1 - Annual FISMA Assessment (FA)
- 3.5.2 - Plan of Action and Milestones (POA&M)
- 3.5.2.1 - Background
- 3.5.2.2 - POA&M Package Components/Submission Format
- 3.5.3 - Timing Requirements for Compliance Conditions
- 3.6 - Security Incident Reporting and Response
- 3.7 - System Security Profile
- 3.8 - Authorization To Operate
- 3.10 - Patch Management
- 3.11 - Security Configuration Management
- 3.11.1 - Security Technical Implementation Guides (STIG)
- 3.11.2 - United States Government Configuration Baseline (USGCB) Standard
- 3.11.3 - National Institute of Standards and Technology (NIST)
- 3.12 - End of Life Technology Components
- 3.13 - Cloud Computing
- *3.14 – MAC ARS Control Tailoring*
- *3.15 - Data Loss Prevention*
- *3.16 - Wireless Access Monitoring*
- *3.17 - Malicious Software*
- *3.18 - Whitelisting*
- *3.19-Data Encryption*

4 - Information And Information Systems Security
- **4.1 - Security Objectives**
- 4.1.2 - Security Level by Information Type
- 4.1.4 - Minimum System Security Requirements—HIGH
- **4.2 - Sensitive Information Protection Requirement**
- **4.2.1 - Restricted Area**

4.2.2 - Security Room
4.2.3 - Secured Area (Secured Interior/Secured Perimeter)
4.2.4 - Container
4.2.4.1 - Locked Container
4.2.4.2 - Security Container
4.2.4.3 - Safe/Vault
4.2.5 - Locking System
4.2.6 - Physical Intrusion Detection System (IDS)
4.2.7 - Minimum Protection Alternatives
4.3 - Encryption Requirements for Data Leaving Data Centers

5 - Internet Security

Appendix A:

1 Introduction

3 Definition of an Acceptable Contingency Plan

4 IT Systems Contingency Planning
4.2 Coordination with Other Business Partners
5 IT Systems Contingency Plan
6 Testing
6.1 Claims Processing Data Centers
6.2 Multiple Contractors
6.3 Test Types
6.3.1 Live vs. Walkthrough
6.3.2 End-to-End
6.4 Local Processing Environments
6.5 Test Planning
7 Minimum Recovery Times
8 Responsibilities
8.1 Business Partner Management
8.2 Systems Security Officer (SSO)
8.3 Service Components (provide support functions such as maintenance, physical security)
8.4 Operating Components (IT operations personnel)
9 Changes
10 Attachments
11 Checklist
12 References

Appendix B:
3 Checklist for Medicare Fraud
Transmittals Issued for this Chapter

Appendices

Appendix A Medicare Information Technology (IT) Systems Contingency Planning

Appendix B An Approach to Fraud Control

Attachments

Attachment 1 Medicare Administrative Contractor Acceptable Risk Safeguards

1 - Introduction

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
This manual addresses the following key Medicare Fee For Service business partner security elements:

- A business partner is a contractor involved in Medicare fee-for-service claims processing
- An overview of primary roles and responsibilities
- A program management planning table to assist System Security Officers (SSOs) and other security staff in coordinating system security programs at business partner sites
- The collection of CMS policies, procedures, standards, and guidelines can be found on the CMS Information Security Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html

The Centers for Medicare & Medicaid Services (CMS) requires that its business partners implement information security controls on their information technology (IT) systems to maintain the confidentiality, integrity, and availability (CIA) of Medicare systems operations in the event of computer incidents or physical disasters.

A CMS business partner (contractor) is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Common Working File (CWF) host sites, standard system maintainers, regional laboratory carriers, claims processing data centers, Data Centers, Virtual Data Centers (VDCs), and Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and Part A/Part B Medicare Administrative Contractors [ABMAC]).

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) - Section 912: Requirements for Information Security for Medicare Administrative Contractors" (Section 912 of the MMA) provided for a new type of contractor relationship, the "Medicare Administrative Contractor," and implemented requirements for annual evaluation, testing, and reporting on security programs at both MACs and existing carrier and intermediary business partners (to include their respective data centers). In this manual, the terms "business partner" and "contractor" are used interchangeably, and all provisions that apply to business partners also apply to MACs. *In addition, the term Acceptable Risk Safeguards (ARS) is used in this manual to mean the ARS that includes the required security and privacy control baselines and tailored with the supplemental controls identified by the Business Owner and ISSO. For the MACs, this will be known as the MAC ARS.*

1.1 - Additional Requirements for MACs

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

MACs are responsible for fulfilling all existing business partner requirements. Additional requirements include the following:

- The contractor shall comply with the CMS MAC tailored list of controls found in Attachment 1. This list of controls*, known as the MAC ARS,* includes all of the CMS required controls plus optional controls *are included* specifically for the MACs. *MAC ARS controls will be tailored via the BPSSM as what is included in the BPSSM overrides the MAC ARS controls with the intent of being more restrictive.*

- The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 days of receipt of the final audit or evaluation report, unless otherwise authorized by CMS.

- The contractor shall document system security controls in the CMS FISMA Controls Tracking System (CFACTS) tool to demonstrate compliance with *MAC* ARS controls and documentation. The contractor shall also use CFACTS to maintain documentation that supports the Authority to Operate (ATO) process, including certification of the documentation.

- The contractor shall conduct or undergo an independent security control assessment of its system security program in accordance with Section 912 of the MMA. The first test shall be completed before the contractor commences claims payment under the contract.

- The contractor shall appoint a Chief Information Officer (CIO) to oversee its compliance with the CMS information security requirements. The contractor's principal Systems Security Officer (SSO) shall be a full-time position dedicated to assisting the business partner CIO in fulfilling these requirements.

- The contractor must implement systems in a manner that is compliant with the CMS eXpedited Life Cycle (XLC) and the Technical Reference Architecture (TRA). When directed by CMS, compliance with the XLC and the TRA will be demonstrated by presenting system updates to the CMS Technical Review Board (TRB). For situations where the TRA conflicts with the *MAC ARS*, the *MAC ARS* shall take precedence.

- *The contractor shall meet all contingency planning and disaster recovery requirements included in the MAC ARS and the Business Partners Systems Security Manual (BPSSM), with the goal of restoring key claims processing and operations within 72 hours.*

- *The contractor shall review, update and approve all policies and procedures every 365 days and not every three years as stated in the MAC ARS.*

2 - IT Systems Security Roles and Responsibilities

2.1 - CMS Contracting Officer's Representative (COR)

CMS CORs oversee the business partners and also have Federal Acquisition Regulation (FAR) responsibilities. The COR has the following responsibilities:

- CMS point of contact for business partner information security problems
- Provider of technical assistance necessary to respond to CMS information security policies and procedures

2.2 - Principal Systems Security Officer (SSO)

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
Business partners shall designate a principal (i.e., primary) SSO qualified to manage the Medicare information security program and ensure the implementation of necessary safeguards. The SSO shall be organizationally independent of IT operations. The SSO can be within the CIO organizational domain but cannot have responsibility for operation, maintenance, or development.

See Section 1.1 for additional requirements that pertain to the Medicare Administrative Contractor SSO position.

The principal SSO position for each contractor should be full-time and fully qualified—preferably credentialed in systems security (e.g., Certified Information Systems Security Professional [CISSP]). Having an individual with appropriate education and experience to execute security administration duties will help reinforce that security must be a cultural norm that guides daily activities, and not a set of compliance directives. A qualified SSO who is available to direct security operations full-time provides the foundation for the security culture and awareness of the organization.

A sound entity-wide security program is the cornerstone of effective security control implementation and maintenance. Security controls cannot be effective without a robust entity-wide security program that is fully sponsored and practiced by senior management, and staffed by individuals with proper training and knowledge. Contractors should also encourage their systems security personnel to pursue security accreditation using available funding.

A business partner may have additional SSOs at various organizational levels, but all security actions that affect Medicare operations shall be coordinated through the principal SSO. The SSO ensures compliance with the CMS information security program and *MAC ARS* by:

- Facilitating the Medicare IT system information security program and ensuring that necessary safeguards are in place and working

- Coordinating information security system activities throughout the organization

- Ensuring that IT system information security requirements are considered during budget development and execution

- Reviewing compliance of all components with the *MAC ARS* and reporting vulnerabilities to management

- Establishing an incident response capability, investigating system security and privacy breaches, and reporting significant problems (see section 3.6) to business partner management.

- Ensuring that technical and operational information security controls are incorporated into new IT systems by participating in all business planning groups and reviewing all new systems/installations and major changes

- Ensuring that IT systems information security requirements are included in Requests for Proposal (RFP) and subcontracts involving the handling, processing, and/or analysis of Medicare data

- Maintaining information security documentation in the System Security Profile for review by CMS and external auditors and keeping all elements of the System Security Profile (see section 3.7)

- Cooperating in all official external evaluations of the business partner's information security program

- Facilitating the completion of the risk assessment (see section 3.2)

- Ensuring that an operational IT Systems Contingency Plan is in place and tested (see section 3.3)

- Documenting and updating the monthly Plan of Action and Milestones (POA&M) (see section 3.5.2). Updates may occur whenever a POA&M projected completion date passes, and/or following the issuance of new requirements, risk assessments, internal audits, and external evaluations.

- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix A)

The principal SSO should earn a minimum of 40 hours in continuing professional education credits each year from a recognized national information systems security organization. The educational sessions conducted at the CMS Security Controls Oversight and Update Training (CSCOUT) can be used toward fulfilling the continuing professional education credits. The qualifying sessions and associated credit hours will be noted on the CSCOUT agenda.

2.3 – CMS Business Owners

Business Owners of business partner systems are responsible for:

- Determining and approving the information and information system security levels of the resources for which they are responsible

- Identifying appropriate security level categorizations for their information and information systems

2.4 – CMS System Maintainers/Developers

Business partner system maintainers/developers have the responsibility to implement the security requirements throughout the eXpedited Life Cycle (XLC).

2.5 - Personnel Security/Suitability

All business partner and contractor employees requiring access to CMS sensitive information shall meet minimum 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. Each position must be evaluated and assigned a risk and/or a sensitivity designation commensurate with each individual's duties and responsibilities. The background check for prospective and existing employees (if not previously completed by CMS) should include, at a minimum: Social Security Number verification, identity and address verification, national criminal database search, county criminal records search, HHS list of excluded individuals, sex offender registry, and verification of academic records.

When required by CMS, the business partner will be expected to support the implementation of Homeland Security Presidential Directive-12. HSPD-12 will require a background check performed by CMS and the ability to support the use of PIV cards, including reading and authenticating an individual with a PIV card, and the passing of PIV credentials to other CMS related networks for authentication.

3 - IT Systems Security Program Management

Key Requirements
The Security Program consists of several fundamental components that are all designed to implement controls and to reduce risk. Key elements of controls include Policies, Procedures, Technical Implementations, Standards, and Management Reviews. Required documentation includes, but is not limited to, the security plan, the risk assessment, and the contingency plan.

Business partners shall implement an IT Systems Security Program to manage the system security risks. Risks are identified by the business partner in the Information Systems Risk Assessment (see section 3.2) and the security requirements are documented in the System Security Plan (see section 3.1). The underlying support for these documents is the controls implemented by the business partner. Controls are measures implemented to protect the CIA of sensitive information. Information security controls shall be implemented in a consistent manner everywhere within the system's accreditation boundary. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. In addition, initial testing shall be performed to ensure that information security controls are operating as intended.

3.01 - Control Components

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Business partners shall have policies and procedures, and implement controls or plans that fulfill the *MAC ARS controls*. The business partner Medicare claims related security program shall be based on the *MAC* ARS *(IOM 100-17, Attachment 1)*, the BPSSM (IOM 100-17) and on the collection of CMS policies, procedures, standards, and guidelines found on the CMS Information Security Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html.

Policies are formal, up-to-date, documented rules that are tailored to the environment, are communicated as "shall" or "will" statements and are readily available to employees. They establish a continuing cycle of assessing risk, implementing controls and monitoring for program effectiveness. Policies are written to cover all major facilities and operations corporate-wide or for a specific asset (e.g., Medicare claims processing), and they are approved by key affected parties. Policies delineate the IT security management structure, clearly assign IT security responsibilities, and lay the foundation necessary to reliably measure progress and compliance. Policies also identify specific penalties and disciplinary actions to be used in the event that the policy is not followed.

Procedures are formal, up-to-date, documented instructions that are provided to implement the security controls identified by the defined policies. They clarify where the action is to be performed, how the action is to be performed, when the action is to be performed, who is to perform the action, and on what the action is to be performed. Procedures clearly define IT security responsibilities and expected behaviors for: asset owners and users, information resources management and data processing personnel, management, and IT security administrators. Procedures also indicate appropriate individuals to be contacted for further information, guidance, and compliance. Finally, procedures document the implementation of, and the rigor with which, the control is applied.

Technical Implementations are the acquisition and installation of hardware, software, or assets to be used for the establishment of a new control, or the improvement of an existing control. The intention of a technical implementation is to automate or facilitate a control process that would otherwise be manually performed.

Standards are formal, written, mandatory actions, rules, or specifications designed to support and conform to a policy or procedure. A standard must include one or more accepted specifications for configurable items for hardware, software, or behavior. Standards are often required to successfully complete technical implementations and can be either part of policies and procedures, or can be standalone documents. Standards can result from, either exclusively by or in combination with, laws promulgated by governing bodies, obtained from known standards organization or developed by the business partner using industry best practices.

Management Review is the business partners' formal oversight activity of control implementations and should be performed at various management levels. Oversight is a regular activity to verify that the control environment for which management has responsibility is functioning properly. Management must set benchmarks or other methods to measure the success of controls. Where appropriate, management should document their review by formally approving evidence supplied.

3.02 - Reporting Requirements

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
Business partners are required to provide documentation to CMS regarding the status of their IT security program. Documentation shall be reported to CMS according to the appropriate procedures, which are summarized in Table 3.1.

Meeting requirements does not validate the quality of a program. Managers with oversight responsibility shall understand the processes and methodology behind the requirements. Table 3.1 identifies key requirements and their high-level descriptions. As appropriate, Table 3.1 refers to other parts of this document that provide details on ways to accomplish each requirement. Business partners shall perform a Federal Information Security Management Act of 2014, 44 U.S.C. §3541 (FISMA) Assessment (FA) using the CFACTS. The weaknesses, action plans, and POA&Ms shall be recorded in the CFACTS (See Risk Management Handbook [RMH] Volume II Procedure 6.2 POA&M Management). To perform the FA, business partners shall conduct a systematic review of the *MAC ARS* using the CFACTS. CFACTS provides the *MAC ARS* guidance and assessment procedures to assist in the review.

In addition, Table 3.1 indicates how often these tasks need to be performed, the disposition of output or documentation, comments, and a space to indicate completion or a "do by" date. The number accompanying each entry in the requirement column indicates the section in this document that deals with that particular requirement. Use this table as a checklist to ensure that all required IT systems security tasks are completed on schedule. Consult the referenced sections for clarifying details.

Table 3.1. Reporting Requirements Planning Table

Requirement	Frequency	Send To	Comments	Complete (check when complete)
CMS POA&M & Annual FISMA Assessment	One third of the controls shall be tested each year so all controls are tested during a 3-year period.	• COR with a copy to CMS CO via CFACTS • System Security Profile	See RMH Volume II Procedure 4.2 for an overview of the FA. FA results recorded in the CFACTS are to be discussed in the Certification Package for Internal Controls (CPIC) Certification Package.	
3.1 System Security Plan (SSP)	The SSP for each General Support System (GSS) and MA shall be reviewed, updated, and certified by management every 365 days, or upon significant change[1].	• CMS CO via CFACTS • System Security Profile	Information system security plans are to be reviewed, updated, and certified by management and indicated as such in CFACTS, the CPIC Certification Package/Statement of Certification, and the System Security Profile[2].	
3.2 Risk Assessment	The risk assessment for each GSS and MA shall be reviewed, updated, and certified by management every 365 days, or upon significant change.[1]	• CMS CO via CFACTS • System Security Profile	Risk assessments are to be reviewed, updated, and certified by management and indicated as such in the CFACTS, the CPIC Certification Package/Statement of Certification, and the System Security Profile. The risk assessment is submitted with the security plan[3].	
3.3 Certification	Each federal FY	• COR with a copy to CMS CO via CFACTS • System Security Profile	Business Partners should include a statement of certification as part of their CPIC package. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-*0*6) information on certification requirements including where, when, and to whom these certifications shall be submitted. All other contractors should submit a statement of security certification to their CMS CORs.	
3.4 Contingency Planning	CPs shall be reviewed, updated, and certified by management every 365 days, or upon significant change.[1] CPs shall be tested annually.	• CMS CO via CFACTS • System Security Profile	Business partner management and the SSO shall approve the CP. The CP is to be developed (in accordance with Appendix A and CMS RMH documents), reviewed, updated, and certified by management—and indicated as such in the CFACTS, the Certification Package/Statement of Certification, and the System Security Profile[4].	
3.5 Compliance	Each federal FY	• ISSO • COR • CMS CO via CFACTS • System Security Profile	POA&M: POA&Ms address findings of internal/external audits/reviews including annual security assessments, and, as applicable: Statements on Standards for Attestation Engagements (SSAE) 1*8* reviews, A-123, Chief Financial Officer (CFO) controls audits, the Section 912 evaluation, and data center tests and reviews.	

[1] NIST defines “significant change” as “any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets.”

[2] More information about system security planning can be found in the CMS Information Security (IS) System Security Plan (SSP) Procedures.

[3] More information about Risk Assessment Reports can be found in the CMS risk assessment procedures.

[4] More information about contingency planning can be found in NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, and NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.

Requirement	Frequency	Send To	Comments	Complete (check when complete)
3.6 Incident Reporting and Response	As necessary	• COR • CMS IT Service desk • Medicare Contractor Management Group (MCMG) Security Mailbox (See the latest guidance from CMS for more information) • System Security Profile	Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file with the Principal SSO		
3.8 Authorization To Operate	As necessary to acquire and maintain a CMS CIO-granted Authorization to Operate.	On file with CMS Information Security and Privacy Group (ISPG), with a copy maintained in the CFACTS.		

LEGEND:

CFACTS	CMS FISMA Controls Tracking System
CFO	Chief Financial Officer
CO	Central Office (CMS)
COR	Contract Officer Representative
CP	Contingency Plan
CPIC	Certification Package for Internal Controls
FA	FISMA Assessment
FY	Fiscal Year
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
MA	Major Application
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SSAE	Statement on Standards for Attestation Engagements
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer

NOTE: The documents listed in Table 3.1 may be stored as paper documents, electronic documents, or any combination thereof.

When submitting paper copies of documentation to the CMS CO, Registered Mail™ or its equivalent (signed receipt required) shall be used. Contact the appropriate COR or ISSO for the correct address.

3.1 - System Security Plan (SSP)

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
Business partners are required to update and re-certify the SSP every 365 days unless there are changes that would necessitate a more frequent update. Updates to the SSP shall be performed via CFACTS.

Defining a system boundary is a key step that must be completed before a SSP can be accurately documented.

The SSP should address how the control environment is implemented to mitigate risks identified in the risk assessment.

The objective of an information security program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process, transmit, or store Medicare-related data have some level of sensitivity and require protection. The protection of a system shall be documented in a security plan. The completion of an security plan is a requirement of the Federal Information Security Management Act of 2014 (FISMA), Privacy Act of 1974, As Amended, Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987. All Medicare claims-related applications and systems categorized as either an MA or GSS shall be covered by security plans.

The purpose of a security plan is to provide an overview of the security requirements of a system and describe the controls that are implemented to meet those requirements. The security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate and cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including Business Owners, information owners, the system operator, and the system security manager (i.e., SSO).

All business partners are required to maintain current security plans for their Medicare claims-related GSSs and MAs in both the CFACTS and their System Security Profiles. The security plan documents the current level of security within the system or application; that is, actual implemented controls, not planned controls. In addition, the security plan serves as the primary documentation reference for testing and evaluation, whether by CMS, the General Accounting Office (GAO), or other oversight bodies. The security plan is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. Therefore, security plans should be distributed only on a need-to-know basis.

The security plans shall be available to the SSO and business partner certifying official (normally the Vice President [VP] for Medicare Operations), and authorized external auditors as required. The SSO and Business Owner are responsible for reviewing the security plan on an annual basis to ensure that it is up-to-date. The objective of these annual reviews is to verify that the controls selected or installed remain adequate to provide a level of protection to reach an acceptable level of risk to operate the system.

All business partner Medicare claims-related security plans shall be developed and documented in accordance with the latest instruction from CMS.

Security plans shall be re-certified within 365 days from the previous certification date. The security plan shall also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update is required. The security plan shall be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review or the updated security plan, if applicable, shall be recorded in the CFACTS, *and* placed in the System Security Profile.

Contractors updating their current security plan(s) or developing new security plan(s) shall take into account Medicare claims processing front-end, back-end, and/or other claims processing related systems.

Front-end systems are those systems Medicare contractors develop and maintain for use in their operations areas and data centers to enter claims and claims-related data into the standard/shared claims processing system. These front-end systems include, but are not limited to: electronic data interchange, imaging systems, optical character recognition, manual claims entry, claims control, provider, beneficiary, other payer databases, and other pre-claims processing business functions.

Back-end systems are those systems that Medicare contractors develop and maintain for use in their operations areas and data centers to output claims processing information (i.e., checks, Medicare summary notices, letters, etc.). These back-end systems include, but are not limited to: print mail, 1099 forms, post-payment medical reviews, customer service, appeals, overpayment written/phone inquiries and separate claims reconciliation systems.

Within 10 days of updating, developing or re-certifying an SSP, CFACTS must be updated.

3.2 - Risk Assessment (RA)

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
Business partners are required to perform an annual risk assessment in accordance with the most current versions of the CMS risk assessment procedures available on the CMS Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html. The identified risks will aid in the design of controls to satisfy the *MAC ARS*.

Documentation of the risks needs to be completed before a control is designed and implemented. Controls should be designed to be cost effective based on the risk to the operating environment.

Risks never go away, but can increase as new vulnerabilities are found and decrease as new or enhanced controls are implemented.

The CMS risk assessment procedures present a systematic approach for the RA process of Medicare information computer systems within the CMS and business partner environments. The procedure describes the steps required to produce a risk assessment for systems and applications.

All business and information owners shall develop, implement, and maintain risk management programs to ensure that appropriate safeguards are taken to protect all CMS resources. A risk-based approach shall be used to determine adequate security and shall include a consideration of the major factors in management, such as the value of the system or application, all threats, all vulnerabilities, and the effectiveness of current or proposed safeguards. The CMS risk assessment procedures shall be used to prepare an annual risk assessment.

Risk assessments shall be re-certified within 365 days from the previous certification date. The risk assessment shall also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update is required. The risk assessment shall be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review or the updated risk assessment, if applicable, shall be placed in the System Security Profile, and a copy shall be submitted to the CMS CO. Note that the risk assessment used to support a security plan cannot be dated more than 365 days earlier than the security plan certification date.

Contractors that must update their current risk assessment(s) shall use the most current versions of the CMS risk assessment procedures.

A newly developed or updated risk assessment that is submitted with the security plan shall be maintained in the CFACTS and must be received within 10 working days after they have been developed and/or updated.

The risk assessment shall be updated every 365 days unless there are changes (as discussed above) that would necessitate a more frequent update. Should risk assessment technical assistance be required, direct all questions to the CMS Information Security and Privacy Group (ISPG) at mailto:CISO@cms.hhs.gov.

3.3 - Contingency Planning

Key Requirements
Business partners are required to document and test an IT Systems Contingency Plan in accordance with the most current versions of the CMS Information Security Contingency Planning standards and procedures available on the CMS Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html, and with BPSSM Appendix A.

All business partners are required to develop and document a Contingency Plan (CP) that describes the arrangements that have been implemented and the steps that shall be taken to continue IT and system operations in the event of a natural or human-caused disaster. Contingency plans shall be included in management planning and shall be:

- Reviewed whenever new systems are planned or new safeguards contemplated
- Reviewed within 365 days to ensure that they remain feasible

- Tested within 365 days. If backup facility testing is done by Medicare contract type (i.e., when multiple contract types are involved [e.g., Data Center, Part A/B, DME]), each individual Medicare contract type shall be tested every 365 days.

Appendix A to this manual provides information on IT systems contingency planning and testing methods. Also, see Table 3.1 for additional information.

Each contractor shall review its CP within 365 days from the date it was last reviewed and/or updated to determine if changes to the CP are needed. A CP shall be updated if a significant change has occurred. The CP shall also be tested within 365 days from the last test performed. Updated plans and test reports (results) shall be maintained in CFACTS, and placed in the contractor's System Security Profile. Business partner management and the SSO shall approve newly developed and/or updated IT Systems CP. Information on Medicare IT systems contingency planning can be found in Appendix A.

A newly developed and/or updated IT Systems CP shall be updated in CFACTS and submitted to CMS within 10 working days after the business partner's management and SSO have approved it. A copy of the IT Systems CP shall be submitted via CD-ROM to the CMS CO along with a paper copy of the statement of certification. This information shall not be submitted via e-mail—Registered Mail™ or its equivalent (signed receipt required) shall be used.

3.4 - Certification

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

All business partners are required to certify their system security compliance. Certification is the formal process by which a contractor official verifies, initially and then by annual reassessments, that a system's security features meet the *MAC ARS controls*. Business partners shall self-certify that their organization successfully completed an annual, independent FA of their Medicare IT systems and associated software in accordance with the terms of their Medicare agreement/contract.

Each contractor is required to self-certify to CMS its information security compliance within each federal FY. This security certification shall be included in the CPIC package or, for contracts not required to submit CPICs, send the security certification to their appropriate CMS CORs. CMS shall continue to require annual, formal re-certifications within each FY no later than September 30, including validation at all levels of security as described in this manual.

Systems security certification shall be fully documented and maintained in the System Security Profile. The security certification validates that the following items have been developed (i.e., updated and/or reviewed, as required) and are available for review in the System Security Profile:

- Certification
- FISMA Annual Security Control Assessment
- System Security Plan for each GSS and MA (see section 3.1)
- Risk Assessment (see section 3.2)
- IT Systems Contingency Plan (see section 3.3 and Appendix A)

- Plan of Action and Milestones (see section 3.5.2)

3.5 - Compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Compliance refers to the contractual obligations of business partners to CMS. The components to electronic data processing (EDP) security reporting compliance are described in detail in the following subsections.

3.5.1 - Annual FISMA Assessment (FA)

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
At least 1/3 of controls must be tested each year, and all controls shall be tested over a 3 year period. CMS reserves the right to identify which control families must be tested each year.

A critical factor for maintaining on-going compliance with FISMA and the Federal Managers' Financial Integrity Act of 1982 (FMFIA) is for Business Owners in coordination with developers/maintainers, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing) and person-hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of applicable POA&Ms for vulnerabilities noted during the annual testing.

The annual FA is documented, tracked, and reported in the CFACTS. The purpose of annual FA testing (i.e., validation) is to examine and analyze implemented security safeguards in order to provide evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. The annual FA is intended to validate the *MAC ARS controls* to determine the extent to which the controls are:

- implemented correctly
- operating as intended
- producing the desired outcome with respect to meeting the security requirements for the system

The annual FA testing requirement has been interpreted by OMB as being within 365 calendar days of the prior test. Over a 3-year period, all *MAC ARS controls* applicable to a system or application shall be tested. This means a subset (no less than one-third [$^1/_3$]) of the *MAC ARS controls* shall be tested each year so that all security controls are tested during a 3-year period. In an effort to standardize testing and results summarization, a 3-year rotation of *MAC ARS* control families was established by CMS. *After the 3-year rotation is completed, the testing rotation shall be repeated until notification from CMS is received.* As control families are added or removed, CMS CO reserves the right to change the controls that must be tested each year.

To fulfill the annual FA validation obligation, the FA shall be conducted by an independent agent or team. This can be any internal/external agent or team that is capable of conducting an impartial

assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain of command associated with the information system or to the determination of *MAC ARS* effectiveness. All management-directed and independent testing conducted with*in* 365 days of the attestation due date may be used to meet the requirement for the annual security controls (i.e., FA) testing.

3.5.2 - Plan of Action and Milestones (POA&M)

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
Business partners are required to prepare a monthly POA&M update which is due by the 1st of each month. The POA&M update consists of updating all active POA&M items in the CFACTS and, if required by CMS, uploading any additional supporting documentation.

All security and privacy related findings shall be entered into CFACTS. This includes findings from FISMA, Chief Financial Officer, Security Control Assessments, penetration tests, Statement on Standards for Attestation Engagement No. 1*8* (SSAE-1*8*) and other reviews and audits.

3.5.2.1 - Background

FISMA requires that federal agencies provide annual reporting of the state of security programs for all IT systems associated with the agency. Additionally, periodic POA&Ms reporting the status of known security weaknesses for all federal agency systems shall also be submitted to the OMB. This reporting requirement applies to a broader scope of security weaknesses, as it is not limited to weaknesses identified by specific audits and reviews (such as those covered under FMFIA). In the case of FISMA, any security weakness identified for any covered system shall be reported and included in a periodic POA&M report.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for MAC business partners (to include their respective data centers). These Section 912 evaluations and reports necessitate an annual on-site review of business partner security programs to ensure that they meet the information security requirements imposed by FISMA and CMS. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified deficiencies (i.e., weaknesses) be addressed in a report to be submitted shortly after the evaluation results are finalized, as well as periodically thereafter to track updated progress towards completion of the identified action plans.

The CFACTS enables contractors to satisfy reporting requirements for security and privacy related findings. Security and privacy related findings and approved action plan data is promptly entered into the CFACTS following all audits/reviews.

3.5.2.2 - POA&M Package Components/Submission Format
(Rev. 11, Issued: 09-30-11, Effective: 10-31-11, Implementation: 10-31-11)

In addition to the initial POA&M reporting that follows each audit/review, summary POA&Ms will be generated on the 1st of each month, based on the data maintained in the CFACTS. The CFACTS shall be populated and maintained with security and privacy related findings and action plans from any audit or review, whether internal or external. Corrective actions are to be established in the CFACTS to address all resulting weaknesses entered therein, and those corrective actions shall be maintained current in the CFACTS to support reporting requirements.

Initial Report. Within 30 days (or as otherwise directed by CMS) of the final results for every internal/external audit/review, an initial CMS POA&M is due to CMS that describes the findings of the audit/review and initial corrective actions planned for implementation.

Monthly POA&M Package. On a monthly basis, business partners shall provide updates in the CFACTS on progress towards completion of remediation efforts for weaknesses identified from all known sources.

3.5.3 - Timing Requirements for Compliance Conditions

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Many security documents, such as risk assessments, security plans, Contingency Plans, as well as many *MAC* ARS control requirements require annual or yearly performance (e.g., test, submission, recertification, review, update). When such a requirement is to be performed annually or yearly, it is to be performed no later than the one year anniversary date of its previous performance (i.e., within 365 days [366 days in leap years]). The only exceptions to this annual/yearly compliance condition are deliverables whose annual due date are set and distributed by CMS, such as the annual FA submission.

If the business partner wishes to change the timing cycle of an annual or yearly requirement compliance date, the business partner is required to shorten the timing cycle and not lengthen the annual/yearly timing cycle to attain the new performance date. For example, if the annual/yearly performance date for reviewing the security plan is 7/31/13 and the business partner desired to change the review date to 5/31/14, they would be required to review the security plan no later than 7/31/13, again no later than 5/31/14, and no later than 5/31/yy thereafter.

For other controls, there may be a requirement they be performed every 6 months, monthly or weekly. To express this in terms of days, every 6 months shall be completed within the range of 181 - 184 days. Monthly controls shall be performed within the range of 28 - 31 days and weekly controls shall be performed within 7 days. The only exception to this is if a monthly or weekly control falls on a non-business day, the control can be completed on the next business day, but the next control process must return to the normal cycle. For example, if a weekly control is normally performed on a Friday, but one Friday is a holiday, the control can be performed on the next business day (i.e., Monday). The control must then be performed again on the upcoming Friday, which would be 4 days later. *If a MAC ARS control is stated in days, then 30 days will be considered a monthly control, and 180 days will be considered a 6 month control.*

Exceptions to the timing requirements can be implemented with the approval of the CMS ISSO. These can be one time exceptions (e.g., a disaster recovery test is performed in 380 days instead of 365 days due to scheduling issues with the recovery facility), or can be for recurring items, as long as the intent of the control is maintained. For example, if a recurring monthly control can be

improved via automation, but alternative timing (i.e., the first business day of each month for a monthly control can vary between 28 and 34 days) must be part of the automation, then the alternative timing can be implemented with the approval of the CMS ISSO.

3.6 - Security Incident Reporting and Response

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
All security incidents shall be reported to CMS in accordance with the requirements listed in the CMS RMH Chapter 8. Incidents shall be reported to the IT Service Desk. *A security incident is a PII or PHI breach, a ransomware event, or an event that impacts the Confidentiality, Integrity or Availability of Medicare data.*

MACs shall email each incident report to mailto:Security_Incident@cms.hhs.gov.

NIST Special Publication 800-61r2 defines a computer security incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet.

The business partner shall use its security policy and procedures to determine whether *a non-reportable event or a reportable* security incident *has occurred. Examples of non-reportable events include a user connecting to a file share, a server receiving a request for a web page, a user sending email and a firewall blocking a connection attempt*. Upon receiving notification of an IT systems security incident or a suspected incident, the SSO or another identified individual shall immediately perform an analysis to determine if an incident actually occurred. The incident could result in adversely impacting the processing of Medicare data or the Confidentiality, Integrity and Availability of Medicare data.

All suspected security incidents or events shall be reported to the business partner's IT service desk (or equivalent business partner function) as soon as an incident comes to the attention of an information system user. All security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS RMH Chapter 8 Incident Response. This document is available on the CMS Information Security Web site at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html. The CMS IT Service Desk can be contacted by

telephone at 800-562-1963 or 410-786-2580, or by e-mail at: mailto:CMS_IT_Service_Desk@cms.hhs.gov. Contacting the CMS IT Service Desk by telephone is recommended if immediate action by CMS is required. *In addition, MACs shall also email each incident report to mailto:Security_Incident@cms.hhs.gov .*

When reporting confirmed security incidents, business partners shall report the date and time when events occurred or were first discovered; names of systems, programs, or networks affected by the incident; and impact analysis. Release of information during incident handling shall be on an as-needed and need-to-know basis. When other entities should be notified of incidents at external business partner sites, CMS will coordinate with legal and public affairs contacts at the effected entities. If a violation of the law is suspected, CMS will notify the Office of Inspector General (OIG) Computer Crime Unit and submit a report to the Federal Computer Incident Response Capability (FedCIRC) of the incident with a copy to the CMS Senior Information Systems Security Office.

As part of the risk management process, the business partner shall determine the extent of the incident's impact and the potential for new or enhanced controls required to mitigate newly identified threats. These new security controls (and associated threats and impacts) should provide additional input into the business partner's risk assessment. Business partners shall refer to The CMS Information Security Incident Handling and Breach Analysis/Notification Procedure for further guidance.

Many of the PII breaches being reported to CMS occur when unencrypted emails are sent to the intended recipients. A mitigating control to allow many of these breaches to be closed more easily is the implementation of the Transport Layer Security (TLS) protocol within email servers such as Microsoft Exchange. The TLS protocol encrypts emails for transmission between two email servers. There are different TLS features which can be used and provide different levels of assurance that an email will be encrypted. Use of any of these features requires TLS to be enabled. To mitigate the severity of email PII breaches, business partners are required to enable TLS on their email servers. In addition, the most secure TLS feature that can be enabled to encrypt emails between business partners shall be implemented. If a business partner cannot implement TLS, a risk must be documented in the RA.

3.7 - System Security Profile

Key Requirements
The System Security Profile is a copy of the documents that are maintained in CFACTS and on CMS Web sites. These documents would be available should business partner management require timely access to them without CFACTS or CMS Web site availability.

Consolidate security documentation (paper documents, electronic documents, or a combination) into a System Security Profile that includes the following items:

- Completed FAs
- Security Plans (for each GSS and MA)
- Risk Assessments

- Certifications
- Contingency Plans
- POA&Ms for each compliance security review
- POA&Ms for other security review undertaken by Department of Health and Human Services (HHS) OIG, CMS, Internal Revenue Service (IRS), GAO, consultants, subcontractors, and business partner security staff
- Incident reporting and responses
- Systems information security policies and procedures

The System Security Profile shall be kept in a secure location, kept up-to-date, and pointers to other relevant documents maintained. A backup copy of the System Security Profile shall be kept at a secure off-site storage location, preferably at the site where back-up tapes and/or back-up facilities are located. The back-up copy of the profile shall also be kept up-to-date, particularly the contingency plan documents.

3.8 - Authorization To Operate

Business partners are required to acquire and maintain a CMS CIO-issued Authorization to Operate (ATO) for each FISMA system. To maintain an ATO, the business partner is expected to maintain all security documentation in CFACTS, and the documentation must be up to date as defined in BPSSM table 3.1. In addition, high risk POA&Ms must be in either a pending verification status or mitigated so the risk can be demonstrated to be moderate or low.

3.10 - Patch Management

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
The timely patching of systems is one of the critical controls to preventing network intrusions.

The *MAC ARS* contain*s* the time frames required to be met for timely patching. The time frame begins when the vendor releases a patch, not when the business partner becomes aware of a patch.

Timely patching is critical to maintaining the operational CIA of Medicare systems. However, failure to keep operating system and application software patched is the most common mistake made by IT professionals. New patches are released daily and it is often difficult for even experienced system administrators to keep abreast of all the new patches. The Computer Emergency Response Team (CERT)/Coordination Center (CC) (http://www.cert.org) estimates the

majority of all network intrusions could be avoided by keeping systems up-to-date with appropriate patches.

To help address this growing problem, CMS recommends that business partners have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. The *MAC ARS* provides specific guidance on time frames for implementing patches. Further guidance is provided in Table 3.3 below for 1) Patch Identification, 2) Patch Installation and 3) Unsupported software.

Table 3.3

Patch Identification	Include all patches that are released from the system, application, or device vendor. All patches must be analyzed by the business partner to determine their applicability and security impact on the operating environment. All patches analyzed from the vendor must be tracked through a formal process and categorized as 1) Security or 2) Operational in nature.
Patch Installation	The *MAC ARS* provides specific guidance on time frames for implementing patches. Security related patches not installed based on business partner analysis shall be documented with an appropriate business justification that includes security impact, operational impact, business impact, mitigating or compensating controls, and residual risk. Re-evaluation of the justification must be performed within every 365 days.
Unsupported Software	Unsupported software, or software that is not formally supported by the software vendor for security or operational patches, shall not be used unless advanced patch support is purchased or provided through another documented source. All unsupported software in operation shall be documented within the Business Partner's IS RA and POA&M with phase out timelines defined.

NIST SP 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program, provides a valuable and definitive process for setting up, maintaining, and documenting a viable patch management process. CMS highly encourages business partners to utilize NIST and other guidance documents to develop configuration standards, templates, and management processes that securely configure Medicare systems as part of their configuration management program.

3.11 - Security Configuration Management

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Key Requirements
Business partners are required to create a security baseline for the configuration of the information system components. A baseline is a formal, management approved standard that documents the customization of guidelines.

Federal guidelines should be used to create baselines. If a Federal guideline does not exist, hardening guides or documented best practices may be used.

DMEMACs, ABMACs, and VDCs are responsible for starting their security configurations with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) Checklists when creating a baseline. All appropriate or referenced DISA checklists and guidelines shall be considered for input into each baseline.

FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. CMS highly encourages business partners to utilize guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

Security configuration guidelines may be developed by different federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or CMS guideline. To resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing Federal security configuration guidelines follows. If there is a conflict between *the MAC* ARS and a DISA STIG, the *MAC* ARS takes precedence. See Table 3.4 for more information. If there are any other questions or concerns about resolving conflicts among security configuration guidelines, business partner SSOs shall contact their CMS ISSO.

Table 3.4

Business Partners	DMEMAC/ABMAC/VDCs
1. *MAC* ARS	1. CMS/*MAC* ARS
2. USGCB	2. DISA/USGCB
3. NIST National Checklist Program (NCP) / NIST	3. NIST National Checklist Program (NCP) / NIST
4. DISA	

3.11.1 - Security Technical Implementation Guides (STIG)

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Security guidelines, called STIGs, are available for most major operating systems, support applications, and infrastructure services. STIGs contain detailed guidance, best practices, and recommendations for configuring a particular product. STIGs are developed by DISA to help system operators configure security within their systems to the highest level possible. DISA also has made available Security Requirement Guides (SRGs) for certain platforms. These guidance

documents may be intended to use along with STIGs as the security guidelines for a specific platform. All STIGs and SRGs are available from DISA. The link for these documents is http://iase.disa.mil/stigs/Pages/index.aspx. CMS recommends that business partner SSOs (or their designated representative) subscribe to the DISA STIG-News Mailing List at: http://iaseapp.disa.mil/stigs/script/subscribe.aspx so they will be notified whenever updated or new STIG Checklists become available.

The use of latest publically available DISA STIG is mandatory for all business partner systems/applications that process, store, and/or transmit Medicare claims data. DMEMACs, ABMACs, and VDCs are required to start with the STIG configurations and then document a customized baseline with any deviations based on environment specific implementation. In the event that DISA does not have a STIG available for a specific platform, business partners should follow the defined CMS hierarchy within the *MAC* ARS controls.

While it may not be possible to implement all of a STIG's recommended security settings because doing so would compromise the functionality of an application and/or system, CMS expects every business partner to analyze the STIG recommended settings and determine which ones are feasible, and to implement all settings that are found to be feasible. Settings that cannot be implemented across an entire platform (e.g. Windows 2008, AIX) shall be documented as "system deviations." Customized baseline values (including those that may already be "system deviations") that cannot be implemented on only specific systems shall be documented as "system exceptions," and settings that cannot be implemented across an entire platform (e.g. Windows 2008, AIX) shall be documented as "system deviations." All STIG recommended security settings that are determined not to be feasible in a business partner environment (including "system exceptions") shall be documented in the applicable system/application Security Configuration Checklist (SCC) with appropriate business justification (security impact, operational impact, business impact), mitigating or compensating controls, and residual risk.

3.11.2 - United States Government Configuration Baseline (USGCB) Standard

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration (FDCC) mandate. While not addressed specifically as the FDCC, the process (now termed the USGCB process) for creating, vetting, and providing baseline configurations settings was originally described in a 22 March 2007 memorandum from OMB to all Federal agencies and department heads and a corresponding memorandum from OMB to all Federal agency and department Chief Information Officers (CIO).

Business Partners have the choice of using the USGCB configurations or the STIGs for the platforms listed on the USGCB Web site at http://usgcb.nist.gov/index.html.

3.11.3 - National Institute of Standards and Technology (NIST)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) tasks NIST to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the federal government."

CMS, as a government agency, highly encourages business partners to review and incorporate the NIST concepts into their Medicare security program. Under the Computer Security Act of 1987 (P.L. 100-235), NIST develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on IT security issues. The publications are issued as Federal Information Processing Standards (FIPS) Publications, Special Publications (SP), NIST Interagency Reports (NISTIRs), and IT Laboratory (ITL) Bulletins.

Special Publications in the 800 series (SP 800-xx) present documents of general interest to the computer security community. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (P.L. 104-106) and the Computer Security Act of 1987 (P.L. 100-235). With the passage of FISMA, there is no longer a statutory provision to allow agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, any reference to a "waiver process" included in FIPS publications is no longer valid. Note, however, that not all FIPS are mandatory; consult the applicability section of each FIPS for details.

CMS does not normally require the verbatim use of NIST SPs for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are specified in this Business Partners Systems Security Manual (BPSSM) and the *MAC* ARS. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop security standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

The most current NIST publications are available at: http://csrc.nist.gov/publications/index.html.

CMS continues to work closely with NIST in the development of new standards, FIPS, and security documentation to ensure the highest and most reasonable level of security of Medicare data.

3.12 - End of Life Technology Components

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

The current HHS policy states "Operating systems, software and applications are considered end-of-life (EOL) when they are no longer supported by the vendor/provider and do not receive product updates and security patches." To align with HHS and beginning with *the MAC* ARS, control SA-22 was added to restrict the use of unsupported information system components. For business partners, components are defined as any hardware or software used by the FISMA system.

While paying for extended support with the component vendor or a third party vendor is acceptable for meeting the HHS policy regarding EOL, business partners are expected to plan for and remove components that are no longer in general support, as soon as possible and within 18 months of the end of general support. General support (defined as mainstream support by Microsoft) for a component starts when the component is made publicly available and ends on the date announced by the vendor. If the component cannot be removed at the end of general support, six months before the end of general support, business partners shall initiate steps appropriate to mitigate any risks (e.g., isolate the component, implement additional monitoring procedures or purchase extended support), document a project plan to remove the component, document the residual risk in the RA and the SSP, and notify their COR if additional support expenses will be incurred. In addition, once the components are no longer in general support, business partners shall work with their federal ISSO and Cyber Risk Advisor to create a POA&M to document and track corrective actions, and document any Risk Acceptances in CFACTS.

3.13 - Cloud Computing

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

According to NIST, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-45). FEDRAMP has implemented security requirements for low, moderate and high risk rank systems. CMS *included* cloud service provider (CSP) controls to ARS version *3.1* for low and moderate systems. Inheritable controls for selected CSPs have been added to CFACTS. MACs and other business partners that are rated as high can use CSPs for non-claims processing functions with the approval of the CMS ISSO. Requirements that are less strict than the *MAC* ARS requirements must still be met, or if not met, must be documented in a CMS Risk Acceptance. Also, other requirements that are not specifically documented in the *MAC* ARS or in an RMH document, such as the reporting of configuration settings is not waived with the use of a CSP; therefore, this should be carefully considered before requesting to use a CSP.

With the publication of FEDRAMP high controls, CMS needs to define the applicable high level controls before any high system can be processed at a CSP. As CMS publishes the high controls, business partners can request to move parts or all of their processing at a CSP.

3.14 – MAC ARS Control Tailoring

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Limited tailoring of certain MAC ARS controls is permissible. The MAC ARS will contain controls that are required to be implemented, but within certain controls, parts of the control can be tailored

to meet appropriate system requirements. For controls where tailoring is permitted, an acknowledgement of the tailoring; and the tailored language, parameter or setting shall be documented in CFACTS within the control implementation section. Any tailoring is subject to review, evaluation and adjustment by CMS to ensure that the intent of the tailored control is met.

Controls that can be tailored include the language identified in the MAC ARS in Table 3: Keyword and Phrases to Identify Tailorable Controls and Control Enhancements.

3.15 - Data Loss Prevention

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Data protection for a Business Partner's environment is critical in ensuring the privacy and integrity of their information. Business Partners must have a comprehensive Data Loss Prevention (DLP) solution in place to provide comfort that data is not being exfiltrated from their environment. The DLP solution should also provide assurance that if unauthorized data exfiltration is identified, it is blocked and the effects are mitigated. The implemented DLP solution must cover data in use (endpoints), data in transit (network), and data at rest (data storage). Several tools implemented for other MAC ARS controls, such as Malicious Code Protection (endpoints), Intrusion Detection System/Intrusion Protection System (network) and encryption (data storage) can be combined to form a DLP solution. Business partners shall maintain documentation to support the DLP solution including formally maintained policies and procedures for the tools, controls, and processes.

3.16 - Wireless Access Monitoring

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

As outlined in MAC ARS AC-18, wireless access to a network is not allowed unless explicitly approved by the CMS CIO. MAC ARS AC-18 also states that an organization must monitor for unauthorized wireless access. Business partners must have a program in place to fulfill this requirement and have associated policies and procedures outlining how the program is operated. The implementation must be capable of identifying unauthorized wireless devices or access points that could be providing access to the network. Monitoring activities should be performed on a periodic basis as needed, but at least quarterly to confirm that unauthorized wireless access does not exist and/or is removed. If wireless access to the environment has been approved by the CMS CIO, an accurate and formally maintained listing of approved access points must be maintained to perform effective monitoring. The approved wireless access point list should be reviewed during the monitoring process to capture necessary updates.

3.17 - Malicious Software

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

MAC ARS SI-3 requires that malicious software mechanisms be in place for an organization's information systems. If malicious software mechanisms are available for a system, they should be

implemented and meet the requirements outlined in SI-3. In the event that an information system/platform does not have compliant malicious software mechanisms available for implementation, the Business Partner should put in place mitigating controls (e.g. file integrity monitoring) to assist in detecting/blocking the risk of malicious software. Documentation for these mitigating controls should be represented in formally maintained policies and procedures specific to the information systems in question.

3.18 - Whitelisting

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

MAC ARS CM-7(5) requires that defined software be documented and explicitly authorized to be allowed to be executed. This authorization of software is known as whitelisting. If the whitelisting of software is a manual process, then the process to review and update the list of authorized software programs must be completed no less often than every seventy-two (72) hours. If automated tools are used to whitelist software, then the automated tools must be updated whenever the authorized software changes or new software is authorized, and the tool must be programmed to either perform a scan the network for unauthorized software no less often than every seventy-two (72) hours, or perform an on-demand evaluation of software every time the software is executed.

3.19 – Data Encryption

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

The MAC ARS includes several controls that require data encryption; however, the language included in some of the controls appears to conflict with language in other controls. To consistently address all of the data encryption controls included in the MAC ARS, a risk assessment shall be completed to determine if the CIA of the data can be maintained with or without encryption. All workstations and portable media containing PII or PHI should already be encrypted. For other hardware and software maintained within the documented and approved system security boundary, where the risk assessment determines that CIA is at risk, FIPS 140-2 compliant encryption shall be implemented for data in transit and/or data at rest. If the risk assessment determines that adequate controls are in place to protect the CIA of the data while it is within the documented and approved system security boundary, then the data can be transmitted and stored in the clear. Also, when encrypting data, the method of encryption can be determined to be hardware or software as appropriate.

4 - Information And Information Systems Security

4.1 - Security Objectives

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

FISMA defines three security objectives for information and information systems: confidentiality, integrity, and availability (CIA). FISMA also directs the promulgation of Federal standards for: (i) the security categorization of Federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category. These Federal standards are issued in the form of FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, respectively.

4.1.2 - Security Level by Information Type

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Using FIPS 199, CMS categorized its information according to information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

CMS has defined many information types processed on and/or by CMS information systems. These information types are defined in the Risk Management Handbooks RMH Vol II Procedure 2-3 Categorizing an Information System and RMH Vol III Standard 3-1 Authentication (for e-authentication), located at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. For each information type, CMS used FIPS 199 to determine its associated security category by evaluating the potential impact value (e.g., High, Moderate, or Low) for each of the three FISMA security objectives—CIA. The resultant security categorization is the CMS System Security Level. This is the basis for assessing the risks to CMS operations and assets, and in selecting the appropriate minimum security controls and techniques (i.e., *MAC ARS controls*).

4.1.4 - Minimum System Security Requirements—HIGH

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

FIPS 200 specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. To comply with FIPS 200, agencies shall first determine the security category (i.e., information type) of their information system in accordance with the provisions of FIPS 199, and then apply the appropriate set of baseline security controls contained in NIST SP 800-53 Rev. 4 (as amended), Recommended Security Controls for Federal Information Systems. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in NIST SP 800-53

Rev. 4. This allows agencies, such as CMS, to adjust the security controls to more closely fit its mission requirements and operational environments.

The CMS Information Security and Privacy Policy contains individual policy statements, along with the CMS Minimum Security Requirements provide technical guidance to CMS and its contractors as to the minimum level of security controls that shall be implemented to protect CMS' information and information systems. These two CMS documents, along with other federal and CMS requirements, form the basis for the *MAC* ARS.

4.2 - Sensitive Information Protection Requirement

Business partners are responsible for implementing the Minimum Protection Standards (MPS) for all CMS sensitive information (digital and non-digital) and information systems categorized at the "HIGH" security level designation. The MPS establishes a uniform method for protecting data and items that require safeguarding. The MPS applies to all IT facilities, areas, or systems processing, storing, or transmitting CMS sensitive information (i.e., any information categorized as "HIGH") in any form or on any media.

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

4.2.1 - Restricted Area

A restricted area is a secured area whose entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas shall either meet secured area criteria or provisions shall be made to store CMS sensitive items in appropriate containers during non-working hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information. All of the following procedures must be implemented to qualify as a restricted area.

Restricted areas shall be indicated by prominently posted signs and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and each entrance shall have controlled access (e.g., electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by a responsible employee positioned at the entrance to enforce the restriction of access to authorized personnel accompanied by one or more officials.

When unescorted, a restricted area register shall be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. Visitors entering the area shall enter (in ink) in the register: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.

The entry control monitor shall verify the identity of visitors by comparing the name and signature entered in the register with the name and signature of some type of photo identification card, such as a driver's license. When leaving the area, the entry control monitor or escort shall enter the visitor's time of departure. Each restricted area register shall be closed out at the end of each month and reviewed by the area supervisor/manager.

To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but are not assigned to the area, an authorized access list (AAL) can be maintained. Each month a new AAL shall be posted and vendors shall be required to sign the register. If there is any doubt on the identity of the individual prior to permitting entry, their identity shall be verified prior to permitting entry.

4.2.2 - Security Room

A security room is a room that has been constructed to resist forced entry. The primary purpose of a security room is to store protectable material. The entire room shall be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, dry wall, etc.) and supplemented by periodic inspection. All doors for entering the security room shall be locked with locking systems meeting the requirements set forth below (section 4.2.5, Locking Systems). Entry is limited to specifically authorized personnel.

Door hinge pins shall be non-removable or installed on the inside of the room. Any glass in doors or walls shall be security glass (a minimum of two layers of 1/8 inch plate glass with .060 inch [1/32] vinyl interlayer, nominal thickness shall be 5/16 inch). Plastic glazing material is not acceptable. Vents and louvers shall be protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciates at a protection console, UL-approved central station, or local police station; and the IDS shall be given top priority for guard/police response during any alarm situation.

Whenever cleaning and/or maintenance are performed, and sensitive systems and/or information may be accessible, the cleaning and/or maintenance shall be done in the presence of an authorized employee.

4.2.3 - Secured Area (Secured Interior/Secured Perimeter)

Secured areas are interior areas or exterior perimeters which have been designed to prevent undetected entry by unauthorized persons during working and non-working hours. Personnel may not reside in computer rooms and/or areas containing sensitive information unless that individual is authorized to access that sensitive information. To qualify as a secured area, the area shall meet the following minimum standards:

- Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, or any lesser-type partition supplemented by UL-approved electronic IDS and fire detection systems.

- Unless electronic IDS devices are used, all doors entering the space shall be locked and strict key or combination control should be exercised.

- In the case of a fence/gate, the fence shall have IDS devices or be continually guarded, and the gate shall be either guarded or locked with intrusion alarms.

- The space shall be cleaned during working hours in the presence of a regularly assigned employee.

4.2.4 - Container

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving, desk and credenza drawers, carts, or any other piece of office equipment designed for the storage of files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide any protection value (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.2.4.1 - Locked Container

A locked container is a commercially available or prefabricated metal cabinet or box with riveted or welded seams, or metal desks with lockable drawers. The lock mechanism may be either a built-in key, or a hasp and lock. A hasp is a hinged metal fastening attached to the cabinet, drawer, etc. that is held in place by a pin or padlock.

4.2.4.2 - Security Container

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks should have only two keys and strict control of the keys is mandatory. If combinations are used, they shall be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files
- Metal lateral files equipped with lock bars on both sides and secured with security padlocks
- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks
- Key lock “Mini Safes” properly mounted with appropriate key control

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

4.2.4.3 - Safe/Vault

A safe/vault is not required for storage of CMS sensitive information. However, if used, they shall meet the following requirements:

- A safe is a GSA-approved container of Class I, IV, or V, or UL listings of TRTL-30 or TRTL-60.
- A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings that uses UL-approved vault doors and meets GSA specifications.

4.2.5 - Locking System

The lock is the most accepted and widely used security device for protecting installations and activities, personnel data, sensitive data, classified material and government and personal property. All containers, rooms, buildings, and facilities containing vulnerable or sensitive items shall be locked when not in actual use. However, regardless of their quality or cost, locks should be

considered as delay devices only and not complete deterrents. Therefore, locking system must be planned and used in conjunction with other security measures.
Minimum requirements for locking systems for secured areas and security rooms are high-security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted deadbolt lock
- Have a deadbolt throw of one inch or longer
- Double-cylinder design; cylinders have five or more pin tumblers
- Contains hardened inserts or inserts made of steel if bolt is visible when locked
- Both the key and lock shall be “off-master”

Convenience-type locking devices such as card keys, sequenced button-activated locks used in conjunction with electric strikes, etc., are authorized for use only during working hours. Keys to secured areas not in the personal custody of an authorized employee and any combinations shall be stored in a security container. The number of keys or persons with knowledge of the combination to a secured area shall be kept to a minimum.

4.2.6 - Physical Intrusion Detection System (IDS)

Physical IDSs are designed to detect attempted breaches of perimeter areas. Physical IDS devices can be used in conjunction with other measures to provide forced entry protection for non-working hour security. Additionally, alarms for individual and document safety (fire), and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical IDS devices include, but are not limited to: door and window contacts, magnetic switches, motion detectors, and sound detectors, that are designed to set off an alarm at a given location when the sensor is disturbed.

4.2.7 - Minimum Protection Alternatives

The objective of the MPS is to prevent unauthorized access to CMS sensitive information. MPS requires two barriers to accessing sensitive information under normal security. The reason for the two barriers is to provide an additional layer of protection to deter, delay, or detect surreptitious entry. Because local factors may require additional security measures, management shall analyze local circumstances to determine space, container, and other security needs at individual facilities.

Table 4.1 shall be used to determine the minimum protection alternatives required to protect CMS sensitive information. Note that any of the three alternative protection standards is acceptable whenever all of the applicable perimeter, interior area, and/or container standards are met. The protection alternative methods are not listed in any order of preference or security significance.

Table 4.1. Protection Alternative Chart

	Perimeter Type	Interior Area Type	Container Type
Alternative #1	Secured		Locked
Alternative #2	Locked	Secured	
Alternative #3	Locked		Security

4.3 - Encryption Requirements for Data Leaving Data Centers

CMS, as a trusted custodian of individual health care data, must protect its most valuable assets—its information and its information systems. Consequently, CMS believes that putting the government's credibility at risk is not acceptable.

No data that includes personally identifiable information (PII) shall be transported from a CMS data center (including business partner data centers and subcontractor data centers) unless it has been encrypted. The only exception to this requirement is for hardcopy records that are transported to and from an off-site location and between off-site locations. To qualify for this exception, the controls listed below (additional information is available from CMS) shall be used.

To prepare the records for shipment:

- The records shall be stored in boxes.
- Each box shall be uniquely identified.
- Boxes shall be secured for shipment.
- Secured boxes shall be loaded into the shipping container or vehicle.
- Total items in each shipment shall be noted and the Bill of Lading signed.
- At time of pickup, the shipping company representative shall verify and sign the Bill of Lading.
- A copy of the identification records shall accompany each shipment.
- The shipping container or vehicle shall be locked and sealed with the seal number noted on the Bill of Lading.
- A copy of the completed Bill of Lading shall be kept by the contractor.

Upon receipt of the shipment at the storage facility:

- A storage facility representative shall verify the seal number and that it is unbroken.
- Compare the contents of the shipment against the Bill of Lading and the boxes against the copy of the identification record.
- If any discrepancies are found, the discrepancy shall be immediately resolved.
- After verification that all boxes shipped were received, information from the Bill of Lading shall be sent to the shipper where it shall be verified.
- Within 24 hours, all boxes on each shipment shall be scanned into the storage facility's tracking system and inserted into the storage racks.

5 - Internet Security

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

With prior written approval of their sponsoring CMS Business Owner, business partners may use Internet technology for transmission of and/or receipt of health care transactions. Each request for using Internet technology will be considered individually and approval is not automatic. However, any approval shall require that business partners meet CMS architectural, security, data interchange, and privacy requirements for Internet-facing infrastructure. Further, an independent (third-party) *Security Control Assessment* of the new functionality prior to its release into production is required and the *Security Control Assessment* must include penetration testing. The *Security Control Assessment* is conducted to validate compliance with the following specific architectural, security, data interchange, and privacy requirements, as well as the *MAC ARS*. The *Security Control Assessment* must be conducted by a CMS-contracted third party. The existing requirement for an annual penetration test of the contractor network shall include any approved Internet infrastructure. Compliance with existing requirements to conduct quarterly vulnerability scans and annual penetration testing is still mandatory.

Briefly, architectural, security, data interchange and privacy requirements include the following:

1. Architecture:

    - Explicit compliance with CMS system lifecycle standards, particularly:
        - CMS Technical Reference Architecture (TRA), as currently released, and all its appendices, and
        - CMS TRA Application Services, as currently released for Application Development Guidelines.
    - Utilization of resources to leverage existing technology and solutions such as platform and software developed by contractors and in compliance with CMS standards to meet the same or similar business requirements. The technology and solutions would also have to align with requirements for the Medicare Administrative Contractors, Enterprise Data Centers, and Standard Front End initiatives.

2. Security:

    - Full compliance with the CMS eXpedited Life Cycle Framework (Checkpoints, Deliverables, and Activities including Security Authorization) in introducing the new functionality.
    - Satisfactory systems test and evaluation of the Internet application to include evaluation of all control categories set forth in the *MAC ARS*.
    - Compliance with DHHS and CMS standard configuration settings.
    - Compliance with the NIST SP 800-41 *Rev. 1*, Guidelines on Firewalls and Firewall Policy; NIST SP 800-44 *Version 2*, Guidelines on Securing Public Web Servers; NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) NIST 800-111, Guide to Storage Encryption Technologies for End User Devices; NIST SP 800-113, Guide to SSL VPNs; NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access; NIST SP 800-115, Technical Guide to Information Security Testing and Assessment; NIST SP 800-119, Guidelines for the Secure Development of IPv6; and NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing.
    - Security Authorization dependent on compliance with security control requirements and completion of documentation such as the risk assessment, the security plan for the

infrastructure, platform, and applications supporting the Internet functionality, and a CP for the supporting platform and application. The risk assessment must address e-authentication requirements and controls for electronic transactions, or refer to a separate document if one exists. All security documentation must be developed to the CMS methodologies and procedures provided at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

3. Privacy: Completion of a Privacy Impact Assessment (PIA) as set forth in Section 208 of the E-Government Act.

4. Data Interchange:

   - Utilization of HIPAA compliance standards for applicable transactions (i.e. claims, remittances and inquiry/response for eligibility and claim status) to be enabled by the new functionality.
   - Enabling both batch file transfer and interactive screen presentation for the HIPAA transactions.
   - 508 compliance for interactive screen presentation.
   - All Internet and non-Internet data exchange modes (i.e. Interactive Voice Recognition, Direct Data Entry, and Computer to Computer) shall return consistent data.
   - Compliance with Trading Partner authentication requirements including submitter/provider relationship for the HIPAA transactions.

Application requirements include but are not limited to the following:

1. A proof of concept/concept of operation paper describing the new application and functionality.
2. Information that the Internet service shall be extended only to entities or providers enrolled in the jurisdiction of the proposing business partner.
3. An attestation that the applicant has had a similar private-side application that has been in production for more than one year. The attestation shall describe the experience of the private-side application and how it relates to the Internet proposal.

Other application requirements may be imposed by the sponsoring CMS business component.

Additionally, business partners may also use the Internet for: 1) utilizing the IRS Filing Information Returns Electronically (FIRE) system for Form 1099 submissions, and 2) utilizing e-mail to transmit sensitive information via encrypted attachments in accordance with all applicable *MAC ARS controls*. An application for these uses is not required. If not already emplaced, contractors must install firewalls, filtering technology to screen incoming e-mail for high risk transmissions such as executables, up-to-date virus protection software, and intrusion detection software to utilize the Internet for these purposes.

Appendix A:
Medicare Information Technology (IT) Systems Contingency Planning

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

Table of Contents

1 Introduction

2 Scope

3 Definition of an Acceptable Contingency Plan

4 Medicare IT Systems Contingency Planning

4.1 Contingency Planning

4.2 Coordination with Other Business Partners

5 Medicare IT Systems Contingency Plan

6 Testing

6.1 Claims Processing Data Centers

6.2 Multiple Contractors

6.3 Test Types

6.3.1 Live vs. Walkthrough

6.3.2 End-to-End

6.4 Local Processing Environments (PCs/LANs)

6.5 Test Planning

7 Minimum Recovery Times

8 Responsibilities

8.1 Business Partner Management

8.2 Systems Security Officer (SSO)

8.3 Service Components (provide support functions such as maintenance, physical security)

8.4 Operating Components (IT operations personnel)

9 Changes

10 Attachments

11 Checklist

12 References

1 Introduction

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

CMS business partners are required by the *MAC ARS* Contingency Planning family to develop and maintain a Contingency Plan (CP). Business partners are expected to develop and test contingency plans that address key recovery scenarios that could occur as the result of a disastrous situation. While a contingency plan cannot address all possible scenarios, the plan should be structured to be useful in a variety of situations. When developing a CP, the business partners are required to address all of the *MAC ARS controls*. The CP needs to be developed in accordance with the CMS RMH VIII 4-4 Standard Contingency Planning document. In addition, NIST Special Publication 800-34 rev 1, Contingency Planning Guide for Federal Information Systems, should be reviewed. NIST identifies different components and plan types that should be documented and be incorporated in a robust CP.

The purpose of this appendix is to supplement the CMS RMH manual and NIST publication and to provide information to aid the business partner in planning for and responding to an emergency or system disruption, and to recover from that emergency or disruption. It is to be used by the CMS Medicare business partner management, IT systems management and staff, and system security persons charged with preparing for continuing the operation of Medicare systems and developing an IT systems CP, or updating an existing plan. In addition, the business partner's SSP and RA should be used as a checkpoint to determine if appropriate contingencies have been addressed in the CP. Also, the CP should be coordinated with the Incident Response activities to address the restoration and recovery activities associated with an incident.

It can be noted that a CP can be out of date shortly after it is created and updated. Automated tools exist to facilitate the development and maintenance of a plan. These tools can significantly help keep a plan current, but they may not address all of the areas required and they may not format the data in a manner that is consistent with CMS requirements. In these situations, the business partner will need to supplement the tools with additional information and cross references to ensure that all required information is documented.

2 Scope

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The business partner IT systems CPs address organizations and sites where Medicare data is processed, including claims processing locations, data centers, and other processing or printing sites.

3 Definition of an Acceptable Contingency Plan

A CP is a document that describes how to deal with an emergency or system disruption. These situations could be caused by, but not be limited to, a power outage, hardware failure, fire, or terrorist activity. A CP is developed and maintained to ensure quick, appropriate, effective, and efficient response in those situations for which a foreseen risk cannot be mitigated or avoided.

Before developing an IT systems CP, it is advisable to have or create a contingency policy. The CP shall be driven by a contingency policy. The contingency policy is a high level

statement relative to what the management wants to do to address a contingency and to recover from the emergency or system disruption.

The IT systems CP shall be developed under the guidance of IT management and systems security persons and all organizational components shall be actively involved in providing information for developing the plan, for making plan related decisions, and for providing support to plan testing.

It can be a very subjective argument relative to what constitutes an acceptable CP. In this document, the description of an acceptable CP is based on the results of the research, analysis and review of various documents from Government and industry, and the review of existing business partner CPs and test reports.

The following summary statements define what constitutes an acceptable CP. This is not an all- inclusive list and the topics are not in any order of importance or priority.

1. Considers the protection of human life as the paramount guiding principle, and then aims at the backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high-quality service.

2. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.

3. Considers risk assessment results.

4. Addresses possible and probable emergencies or system disruptions that would require the implementation of the CP.

5. Can be sufficiently tested on an established regular basis within recommended recovery periods at reasonable cost.

6. Contains information that is needed and useful during an emergency or system disruption.

7. Can, when implemented, produce a response and recovery, such that critical business functions are continued.

8. Specifies the persons necessary to implement the plan, and clearly defines their responsibilities.

9. Clearly defines the resources necessary to implement the plan.

10. Reflects what can be done – is not a wish list.

11. Assumes people shall use sound judgment, but will need clearly stated guidance, since they will be functioning in a non-normal environment, under possibly severe conditions and pressure.

12. Addresses backup and alternate sites.

13. Addresses the use of manual operations, where appropriate and necessary.

14. Contains definitive “Call Lists” to use for contacting the appropriate persons in the proper sequence. These lists would include vendor points of contact.

An acceptable CP should be straight to the point. It should not contain any more information than is necessary to plan for and implement contingency actions. The users should not get bogged down in detail as they read the plan to determine what to do, when to do it, what is needed to do it, and who should do it. The CP should serve as a “user’s manual” and be easy to understand and use.

Because a CP is designed to be used in a stressful situation, it shall be written with that as a foremost thought in mind. The prime objective is to maximize the continuity of critical operations.

Reviewing a CP and testing it will help determine whether it remains an acceptable plan. The review and testing shall not focus solely on content, but shall also focus on ease of use.

A complete set of CPs for an organization may be made up of several smaller CPs, one for each business function (e.g. claims processing) or for a single data center, for example. This breakdown into manageable parts helps to keep a plan easy to use.

Careful thought should be given to the organization of the CP. The organization should be logical in terms of what will the user want to know or do first. If the first thing that should happen in an emergency is that a call list shall be used to notify persons, then that call list, or a pointer to it, should be placed very near the front of the CP. Not every informational item to be utilized during a contingency event will be in the CP document. For example, the plan may point to an attachment or to a separate procedures manual. It is imperative to assure that any information provided in a separate procedures manual is readily available and easily obtainable. In this regard, a CP should contain a very understandable and useful table of contents, so that a user can quickly find the information being sought.

Contingency planning can provide a cost-effective way to ensure that critical IT capabilities can be recovered quickly after an emergency. IT systems contingency planning shall embrace a coordinated contingency policy of what will be done to fully recover and reconstitute all operations.

4 IT Systems Contingency Planning

The goal of IT systems contingency planning is to continue accomplishing critical IT systems operations in an emergency or system disruption and to accomplish a rapid and smooth recovery process.

4.1 Contingency Planning

Contingency planning is preparing for actions in the event of an emergency situation, and giving some thought and planning to what your organization will do to respond and recover. The IT systems contingency planning process shall address all the actions and resources needed to ensure continuity of operation of critical IT systems and the means of implementing the needed resources. IT management and staff shall be trained to handle emergency or system disruption situations in data centers and other areas where data processing systems are located.

Contingency planning includes such training.

It is advisable to establish a IT systems contingency planning team. This team would be responsible for defining critical IT systems, including applications software, data, processing and communications capabilities, and other supporting resources. These would be the key people in the implementation of the plan.

4.2 Coordination with Other Business Partners

If a business partner's data center or other data processing environment is linked to other business partners for the transmission of Medicare data, then the contingency planning shall address those links relative to receiving input, exchanging files, and distributing output. If alternate/backup IT systems capabilities are to be utilized, then their functions and data transmission links shall be considered in the planning.

Coordination with other business partners is essential to completing the IT systems contingency planning process.

5 IT Systems Contingency Plan

The following format in conjunction with the RMH may be used in developing a IT Systems CP. While this format is not required, all of its elements shall be included in the CP.

1. Introduction
   - Background
   - Purpose/Objective
   - Management commitment statement
   - Concept of operations
   - Scope
     - Organizations
     - Systems
     - Boundaries
   - IT capabilities and resources
   - CP policy
     - Priorities
     - Continuous operation
     - Recovery after short interruption
   - Minimum recovery times

2. Assumptions

3. Authority/References

4. Definition of what the CP addresses
   - Organizations
   - Systems
   - Boundaries

5. Three phases defined

- Respond
- Recover
- Restore/reconstitute

6. Roles/Responsibilities defined

7. Definition of critical functions

8. Alternate capabilities and backup

9. Definition of required resources to respond and recover

10. Training
    - CP shall address Who – When – How

11. Testing the CP
    - Philosophy
    - Plans
    - Boundaries
    - Live vs. Walkthrough
    - Reports
    - Responsibilities

12. CP maintenance/updating
    - Schedule

13. Relationships/Interfaces
    - Outside (vendors, providers, banks, utilities, services, CMS)
    - Internal
    - Dependencies

14. Attachments
    - Actions for each phase
    - Procedures
    - Call trees
    - Vendor contact list
    - Hardware inventory
    - Software inventory
    - System descriptions
    - Alternate/Backup site information
    - Assets/Resources
    - Risk Assessment Summary (refer to System Security Plans)
    - Agreements/Memos of Understanding
    - Manual Operations
    - Supplies/Materials/Equipment
    - Floor plans
    - Maps

The CP shall provide for off-site storage:

- Backup software
- Data
- Appropriate documents (emergency telephone lists, memos of understanding, etc.)
- Copies of the CP
- Administrative supplies (forms, blank check stock, etc.)

6 Testing

CMS requires testing of the CP annually under conditions that simulate an emergency or a disaster. A CP shall also be tested after a substantive system change that necessitates a revision to the CP.

CMS requires that the critical IT systems shall be tested within every 365 days and the CP updated to accommodate any changes, including updated versions of software or critical data. Critical systems are those whose failure to function, for even a short time, could have a severe impact, or have a high potential for fraud, waste, or abuse.

6.1 Claims Processing Data Centers

Many of the contractors with which CMS has direct contracts do not have their own data centers. They usually contract this service out. If a business partner does not have its own data center, then it is the responsibility of the business partner to inform the subcontractor that operates the data center that they shall have a CP that addresses the requirements outlined in the Appendix.

6.2 Multiple Contractors

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Data centers usually serve multiple contractors. Existing shared processing environments allow for multiple contractors to process claims at a data center. There are numerous data centers processing Part A and Part B claims for multiple Medicare contractors.

It is important to test a CP at a data center that serves multiple contractors. This provides a mechanism to examine the possible commingling of data between contractors, wherein data may be compromised.

Before testing of the CP begins, it is important to understand how contractor data is protected and/or kept separate. The data centers may use a security package, such as ACF, to control access and separation of data. In order to perform appropriate testing, the complexity of the data center operation must be understood.

6.3 Test Types

CP test guidance suggests four types of testing:

- Walkthrough/Tabletop Test
- Checklists
- Simulation/modeling
- Tabletop Test
- Live/Comprehensive Exercises

These are defined below:

- **Walkthrough/Tabletop Test**: A walkthrough test is accomplished by going through a set of steps to accomplish a particular task or action initiated because of a contingency event. The precursor to a walkthrough test is that the steps are documented so that they can be logically followed. A "test team" might sit around a table and talk through each step and then walk through" the various steps, and then discuss expected outcomes and further actions to be taken. They may use a checklist to ensure that all features of a step are addressed or that all resources necessary to accomplish the task or action are considered. A walkthrough test does not involve accomplishing the actions being tested in real time or using the live environment. A walkthrough test could be accomplished by using a group of test people to act out what might happen if a real contingency event occurred. They might go to the alternate site, but they would not actually start all hardware, software, and communication operations in order to assume the function of the primary site.

  For those applications that are both hosted at CMS and not participating in a broader recovery test to a CMS-approved recovery site during their annual test cycle, a tabletop test is required. A tabletop test is discussion-based only, and does not involve deploying equipment or other resources. The discussion during the test can be based on a single scenario or multiple scenarios. By simulating an emergency in an informal, stress- free environment, this test method allows for the free exchange of ideas and provides participants an opportunity to practice the steps to be followed in an actual event and to identify areas in the CP for enhancement.

  A successful tabletop test steps participants through real-life scenarios; captures its results in a formal report; and incorporates the "lessons learned" into subsequent versions of the CP and the tabletop test plan. Refer to CMS Contingency Planning Tabletop Test Procedures, for step-by-step instructions for conduction a tabletop test.

- Checklists: Checklists are used to clearly present a step-by-step logical sequence so systems and sub-systems may be recovered in a logical manner. Checklists are intended to provide a direct, simple coordinated listing of events that ensure that all necessary steps are executed during the recovery process.

- **Simulation/Modeling**: Modeling involves creating a computer model of the process to be tested. This allows easy testing of many variables without physically having to make changes. For example, you can vary the number of servers that go down during a disaster or the number of people that can get to an alternate site following a disaster.

  Simulation involves taking physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team does

the same at the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.

- **Live/Comprehensive Exercises**: This is the most complete and expensive test to accomplish. It involves completing the physical steps that would actually be taken if an emergency occurred. People and materials would be moved to an alternate site for the test, and servers would actually be shut down to reduce capability. Power would be shut off, and live conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications, and people at the alternate site would be set into action and begin functioning as the primary site to support operations.

End-to-end refers to the scope of the testing (partial testing is less than end-to-end).
When conducting end-to-end testing, items to consider include:

- End-to-end testing can be completed as part of walkthrough or live test.
- Not testing end-to-end means that some links, processes, or subsystems are missed.
- What is the risk in not conducting end-to-end testing?
- Live end-to-end testing can be very expensive!

Considering risks and cost, management shall make a decision as to what type and scope of testing is appropriate.

6.3.1 Live vs. Walkthrough

- High-level testing can take the form of a walkthrough test.
- A walkthrough can be part of the overall testing process, but not the whole process.
- Lower-level testing can include a walkthrough, if live testing is not an option.
  - Live testing shall be the first choice.
  - Fall back to a simulation/model if live testing is not an option.
    Cost, time, and interruption of normal operations are major considerations in doing a live test.
  - A walkthrough test should be the last resort.
- Consider what a walkthrough test would miss.
- Consider the ramifications of missing that part of the test.
- Remember that there is risk in not doing a live test—is the risk acceptable?
  - Consider the criticality of functions, processes, and systems.
    If critical to continuing essential business operations, then these are strong candidates for live testing.

- Testing interfaces.
  It is important to test the critical interfaces with internal and external systems. It is difficult to test interfaces using a "walkthrough" method. Simulation or "live" testing is preferred.

- Cost and complexity.
  The decision as to how to test critical functions, processes, and systems must result from careful consideration of complexity and cost. A complete "live" test of all elements of an operation may prove to be extremely costly, in terms of both dollars and time. If that cost outweighs the "cost" of the risk of not doing live testing, then "live" testing should probably be ruled out.

6.3.2 End-to-End

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

This kind of testing aims to ensure that all software and hardware components associated with a function, process, or system are tested from the front end through to the back end (input through process through output). As with live testing, end-to-end testing can be expensive.

- End-to-end testing shall only be considered for critical functions, processes, or systems.

- Why is end-to-end testing needed?

- It provides the best assurance that there are no problems.

- Would a partial test be meaningful?
  If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical ones need be considered for end-to-end testing.

- Examples of types of end-to-end tests:
  - Claims receipt through to check generation
  - Query of a database through to the response
  - Medicare Secondary Payer (MSP) check request through to check issue and back to MSP

- Evaluate complexity and cost.
  The decision on how to test critical functions, processes, and systems shall carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and time. If that cost outweighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.

- Consider the criticality of functions, processes, and systems.
  Look at the criticality of functions, processes, and systems. If these are critical to continuing essential business operations, then these are strong candidates for end-to-end testing.

- If you cannot do end-to-end testing, then consider live testing of all links possible to

help ensure minimum problems.
- Or, do simulation/modeling
- Or, do walkthrough

Overall testing may take the form of reviews, analyses, or simulations of contingencies. Reviews and analyses may be used for non-critical systems, whereas critical systems shall be tested under conditions that simulate an emergency or a disaster.

It is advisable that the testing of critical systems be done end-to-end, input through output, so that no physical activity, automated process, or Medicare business partner system is left untested. Critical interfaces internal and external to the systems shall be tested.

Testing may include activities in addition to computer processing. Manual operations shall be checked according to procedures, and changes made as experience indicates.

6.4 Local Processing Environments

IT systems CP testing relative to local environments, such as individual or clustered workstations and local area network (LAN) configurations, may be less comprehensive than data center testing. Reviews and analyses may be used to accomplish certain non-critical systems testing, whereas critical systems require full simulation or live testing. The criticality of the system is the deciding factor relative to what type testing is used, how often tests are accomplished, and how thorough the testing shall be.

The decision of which test approach to use relative to a specific system or configuration shall be a management decision based on advice from the System Security Officer (SSO), IT systems staff, operations and support representatives, and the lead test planner/manager.

6.5 Test Planning

An IT systems contingency test plan shall address at least the following:

- Test objectives
- Test approach
- Required equipment and resources
- Necessary personnel
- Schedules and locations
- Test procedures
- Test results
- Failed tests
- Corrective action management process
- Retest
- Approvals

It is advisable to establish test teams responsible for preparing and executing the IT systems CP tests. Responsibilities shall be assigned to test team members, including executives, observers, and contractors.

Following testing, the corrections specified in a Corrective Action Management Process shall be

tested. The process shall include:

- List of items that failed the previous test
- Corrections planned
- Retest detail
- Schedule
- Review responsibilities

Ensure that the lessons learned from IT systems CP testing are formally discussed among senior business partner management, operations, IT management and staff, and the SSO.

Documentation shall exist for:

- Test plans
- Test results
- Corrective action management process
- Retest plans
- Memos of Understanding/Formal Test Arrangements
- Lessons Learned

7 Minimum Recovery Times

Maximum Tolerable Downtime (MTD) is the time it takes to recover an operation, function, process, program, file, or whatever has to be recovered as an operational entity.

Minimum recovery time is the longest acceptable period of time for recovery of operations. If claims processing operations must be recovered within 72 hours, then that is the MTD to recover. Anything over that is unacceptable.

- Recovery times may vary, depending on the criticality of the entity involved.
- Times can be from a few minutes to days or weeks.
- A table/matrix can be constructed that lists the recovery times.
- There can be a separate table/matrix for each organization or major function (e.g., claims processing, medical review, check generation).
- Recovery times shall be carefully defined and must be achievable.
- Recovery times shall be verified to some extent through testing (simulation or live).

8 Responsibilities

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Following is a summary of responsibilities for key groups and persons involved with contingency planning.

8.1 Business Partner Management

- Defines scope and purpose of IT systems contingency planning.
- Authorizes preliminary IT systems contingency planning.
- Ensures that appropriate CPs are developed, periodically tested, and maintained.
- Ensures that all IT operations participate in the contingency planning and the development of the plans.
- Reviews the plan and recommendations.
- Requests and/or provides funds for plan development and approved recommendations.
- Assigns teams to accomplish development of test procedures, and for testing the plan.
- Reviews test results.
- Ensures that the appropriate personnel have been delegated and notified about the responsibility for effecting backup operations, and that the backup copies of critical data are ready for use in the event of a disruption.
- Ensures that the business partner organization can demonstrate the ability to provide continuity of critical IT systems operation in the event of an emergency.
- Business partner management shall approve:
  - The CP
  - Changes to the CP
  - Test Plans
  - Test results
  - Corrective action management processes
  - Retest Plans
  - Memos of Understanding/Formal Arrangement Documents
  - Lessons Learned
  - Changes to storage and backup/alternate site facilities

8.2 Systems Security Officer (SSO)

- Documents the scope and purpose of IT systems contingency planning
- Reconciles discrepancies and conflicts
- Evaluates security of backup and alternate sites
- Leads the preparation of the CP
- Submits the plan and recommendations to management
- Monitors implementation of the plan and reports status to management
- Ensures all testing of the plan is accomplished as required
- Reviews test results
- Ensures that the plan is updated based on test results
- Ensures lessons learned are formally documented and discussed

8.3 Service Components (provide support functions such as maintenance, physical security)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

- Maintain physical security forces to respond to emergencies.
- Schedule fire and other emergency drills and monitor effectiveness.
- Develop emergency re-supply procedures for forms, supplies, equipment, and furniture.
- Provide for priority replacement of computer hardware.
- Provide for restoring telecommunications.
- Provide for backup sites and procedures.
- Provide information relative to the availability of recovery sites.
- Develop procedures for documenting inventories of equipment and furniture.
- Provide a list of employees' home addresses and phone numbers.
- Support testing of the plan.

8.4 Operating Components (IT operations personnel)

- Designate employees for emergency response teams.
- Designate employees for backup teams.
- Designate employees for recovery teams.
- Provide a list of employees' home addresses and phone numbers.
- Identify time-critical operations and systems.
- Identify critical resources, such as hardware, software, data, communications, facilities, and people.
- Identify supplies (forms, blank check stock, etc.) to be stored at alternate sites.
- Identify processes for obtaining items stored at alternate sites.
- Identify critical data to be backed up offsite.
- Provide information on testing requirements.
- Accomplish and/or support end-to-end system testing.
- Review test results.
- Identify critical, non-automated data processing operations.
- Review basic service organization plans and advise SSO where needs are not met.
- Monitor CP implementation and report status to management.

9 Changes

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The CP shall be updated whenever one or more of the following events occurs:

- New systems or operations added.
- Upgrade or replacement of Standard System software.
- Hardware or software replacement.
- Changed back up/alternate site.
- Changed storage facilities.
- Removal of existing systems or operations

10 Attachments

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Materials that are too extensive to be included in the body of the Medicare IT Systems CP shall be included as attachments. These shall be referenced in the contingency plan. These shall also be a part of the System Security Profile. Existing material that facilitates response, backup, and recovery operations shall be included as attachments or a pointer provided. Much of this material is bulky and relates to the entire organization. The SSO shall ensure that the information to be attached is pertinent and current, and that updated copies are routinely incorporated, particularly into offsite copies of the CP. Such material includes:

- Master inventories of forms, supplies, and equipment
- Description of computer hardware and peripherals
- Description of applications software
- Appropriate security weakness information
- Systems and program documentation
- Prioritized schedules for computer operations
- Communications requirements, especially computer networks

11 Checklist

The following checklist provides a means for determining if a CP contains the appropriate information that can readily be used in handling an emergency or system disruption. This list is not all-inclusive, but rather should serve as a thought stimulus for evaluating CPs.

This checklist uses the same outline as the suggested CP format.

1. Introduction
   Does the CP contain:

   - Background
     Is a history of the plan provided? Are the physical environment and the systems discussed?

   - Purpose/Objective
     What does the plan address? Why was it written? What does it aim to accomplish?

   - Management Commitment Statement
     Has the CP been approved by management and the SSO? Once the CP is created, reviewed, and ready for distribution, it shall be approved by site, operations and information systems management, and the SSO.

   - Scope

     Are the boundaries of the plan indicated? What organizations are involved, not involved?
     - Organizations
     - Systems
     - Boundaries

- External Interfaces

- IT Capabilities and Resources

  Is the focus of the plan on IT systems, capabilities, and resources?

- CP Policy

  - Priorities
    - Are the CP steps ranked according to priority?

  - Continuous Operation
    - Are there functions, processes, or systems that are required to continue without interruption?

  - Recovery after Short Interruption
    - Which functions, processes, or systems can be interrupted for a short time?

  - Recovery Times?
    - Are the recover times stated?
    - What are the minimum recovery times?

  - Standalone Units
    - Does a CP exist for any standalone workstation? A key part of a CP shall address any standalone workstations that are part of the critical operations environment. It shall state where backup software and support data for these workstations is stored.
    - Is the plan reviewed and approved by other key affected persons?

2. Assumptions

   Are all the important assumptions listed? Have the assumptions been carefully reviewed by the appropriate persons to ensure their validity?

3. Authority/References
   - Who or what document is authorizing the creation of the CP?
   - What are the key references that apply to the plan?

4. Definition of what the CP Addresses

   - Organizations

     To which organizations does the CP apply?

   - Systems

     Is there a general description of systems and/or processes?

   - Boundaries

     Are the system boundaries clearly defined?

   - External Interfaces

     Are external interfaces clearly defined?

5. Three phases defined
   Does the plan address three phases of emergency or system disruption?

   - Respond
     - Is this phase adequately described so that it is understood what activities occur therein?
     - Are people, and their safety, considered?
     - Is damage/impact assessment considered?
     - Are the alerting and initial impact assessment procedures fully explained as well as arrangements for continual review of their use and effectiveness?

   - Recover
     - Is this phase adequately described so that it is understood what activities occur during this phase?
     - Are effective recovery strategies in place for hardware, software and data?
     - Are hardware configuration and operating system requirements considered?
     - Have interdependencies between internal and/or external systems considered?

   - Restore/Reconstitute
     - Is this phase adequately described so that it is understood what activities occur during this phase?
     - Has validation of data been documented?
     - Has a clear path for validating system functionality and operational capabilities been implemented?

6. Roles/Responsibilities Defined

   - Has the necessary CP implementation organization been defined and the responsibilities of all those involved clearly stated with no 'gray areas'?

   - Will all who have a task to perform be aware of what is expected of them?

   - Does the CP assign responsibilities for recovery? The responsibilities of key management and staff persons shall be carefully described in the CP, so that there is no question relative to the duties of these people during an emergency.

7. Definition of Critical Functions

   - Does the CP address critical systems and processes?

   - Have emergency processing priorities been established and approved by management?

   - Does the CP specify critical data? The CP shall specify the critical data needed to continue critical business functions and how frequently the data is backed up.

   - Has a list of critical operations, data, and applications been created? In preparing the CP, a list of current critical operations, data and applications shall be documented and approved by management. This list shall contain the items needed to continue the minimum critical business elements and functions until operations could be returned to a normal mode.

8. Alternate Capabilities and Backup

- Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.

- Does the CP address issues relative to pre-planned alternate locations? The CP shall address any potential issues relative to pre-planned alternate locations. These include:
  - insurance
  - equipment replacement
  - phones
  - utilities
  - security

- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities shall include:
  - prioritizing operations
  - identifying key personnel and how to reach them
  - listing backup systems and where they are located
  - stocking critical forms, blank check stock, and supplies off-site
  - developing reliable sources for replacing equipment on an emergency basis

- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?

- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?

- Have temporary data storage sites and location of stored backups been identified?

- Is the frequency of file backup documented?

- Have the arrangements been made for ensuring continuing communications capabilities?

- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?

- Are system, application, and other key documentation maintained at the off-site location?

- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?

- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs. These are stored at off-site locations sufficiently distant from the primary site so as not to be affected by the same emergency that would affect the primary site.

- Is the CP stored off-site at alternate/backup locations? Copies of the CP shall be stored

at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the CP that are stored in a private home shall be protected from inadvertent access.

9. Required Resources

- Are the following resources for supporting critical operations defined and available for an emergency?
  - Hardware
  - Software
  - Communications
  - Data
  - Documents
  - Facilities
  - People
  - Supplies
  - Basic essentials (water, food, shelter, transportation, etc.)

- Does the CP provide for backup personnel? As the CP is implemented, it is necessary to have additional people available to support recovery operations. The CP shall specify who these people are and when they would normally be called into action.

10. Training

- Are management and staff trained to respond to emergencies? Security training shall include modules for management and staff relative to their roles for handling emergency situations.

11. Testing the CP

- Is there a section in the CP that addresses testing of the plan?
- Testing of the CP shall address the following topics:
  - Test Philosophy
  - Test Plans
  - Boundaries
  - Live vs. Walkthrough vs. End-to-End Testing
  - Test Reports
  - Responsibilities

12. CP Maintenance

- Schedule
  - Is the CP annually reviewed and tested within every 365 days? The CP shall be reviewed and tested under conditions as close to an emergency as can be reasonably and economically simulated.
  - Is there a provision for updating the CP within every 365 days?
  - Is the CP revised after testing, depending on test results? Are lessons learned documented and incorporated into the revise CP?

13. Relationships/Interfaces

- Does the CP identify critical interfaces? Interfaces required to continue critical

business functions should be identified. Refer to the System Security Plans.

- Which outside (vendors, providers, banks, utilities, services, CMS) interfaces must be considered?
- Is the plan compatible with plans of interacting organizations and systems?
- What internal interfaces must be considered?
- Which corporate interfaces must be considered?
- Are there special interfaces with corporate systems that must be addressed in the CP?

14. Attachments

Does the CP contain appropriate attachments, as listed below?

A. Actions for Each Phase

Are the actions to be taken in each phase (respond, recover, restore) of the contingency clearly described and related to organizations and/or people?

B. Procedures

- Are there detailed instructions for:
  - responding to emergencies?
  - recovering operations?
  - restoring operations?
- Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency shall be in place.
- Are there procedures for addressing the situation where the processing site is intact, but people can't get to it because of a natural disaster? Can the business be operated remotely?
- Is there an implementation plan for working from home?

C. Call Trees

Are there call lists with names, addresses, and phone numbers with priority order relative to whom to call first?

D. Hardware Inventory

Are there lists of all the hardware covered by the CP?

E. Software Inventory

Are there lists of all the software covered by the CP?

F. System Descriptions

Are all the systems covered by the CP defined, including appropriate diagrams?

G. Alternate/Backup Site Information

Is there sufficient detail to completely describe the alternate and/or backup sites, including addresses, phone numbers, contacts, resources available at the sites, and, resources needed to be brought to the site?

H. Assets/Resources

Are there lists of all the needed resources for responding, recovery, and restoring operations?

I. Risk Assessment Summary

Has there been a realistic assessment of the nature and size of the possible threat and of the resources most at risk?

J. Agreements/Memo of Understanding

Are there agreements in place relative to the use of alternate/backup sites, special resources, outside suppliers, extra people, alternate communications, etc?

K. Manual Operations

Are manual operating procedures in place so that certain functions can continue manually if automated support is not available soon enough?

Manual processing procedures shall exist in the backup phase until automated capabilities can take over the information processing. Provisions shall be made to provide this manual capability.

L. Supplies/Materials/Equipment

Is there information that describes how and where to obtain needed supplies, materials, and equipment?

M. Floor Plans

Are the necessary floor plans available?

N. Maps

Are the necessary area and street maps available?

12 References

In addition to this manual, the following documents may be referenced during the IT systems contingency planning process:

- NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Information

Technology Systems, May 2010.
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1.pdf

- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 11.
  http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

- Health Insurance Portability & Accountability Act (HIPAA): The Race to Become Compliant, Ed Deveau, Disaster Recovery Journal, Fall 2000.

- Federal Information System Controls Audit Manual (FISCAM), Exposure Draft, GAO-08-1029G, Section 3.5.
  http://www.gao.gov/new.items/d081029g.pdf

- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.
  http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html

- Office of Management & Budget, Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, 8 February 1996.
  http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

Appendix B:
An Approach to Fraud Control

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Table of Contents

1 Introduction

2 Safeguards against Employee Fraud

3 Checklist for Medicare Fraud

1 Introduction

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

This document develops countermeasures relating to fraudulent acts and a checklist to help Medicare contractors assess their vulnerability to fraud. Fraud and embezzlement are skyrocketing, largely because basic safeguards are neglected or lacking. Fraudulent acts are discussed in terms of the types of safeguards in place and functioning.

2 Safeguards against Employee Fraud

(Rev. 14, Issued: 06-15-18), Effective: 11-30-18, Implementation: 11-30-18)

The following safeguards are specific countermeasures against fraudulent acts by employees whose functions involve Medicare program funds. These safeguards are consistent with the *MAC* ARS, and do not constitute wholly different or additional minimum requirements. The following countermeasures should prove especially effective against currently prevalent fraudulent activities and are discussed primarily as they relate to prevention and detection of fraud.

A. Screen New Employees

Screen new employees for positions that involve program funds directly or indirectly to address the applicant's past faithful and honest performance of duties with other employers in addition to job performance and investigation of his/her personal finances. New employees' statements concerning personal finances shall be confirmed with former employers and with banking and credit institutions. Phone calls to previous employers are essential, particularly to former supervisors who should be advised of the nature of the position. Although former employers will sometimes fail to prosecute employees associated with fraudulent activities, they seldom delude a prospective employer asking about the applicant’s integrity.

Any blatant dishonesty in the application (such as claiming qualifications and experience the applicant never had) shall remove the applicant from further consideration. Check references and crosscheck them (one against the other) for consistency as well as content. Evaluate references on the basis of the contact's personal knowledge of the applicant's job-related qualifications and integrity.

Proper screening is preventive medicine at its best. Gaps in employment are flags that call for third-party verification, not just a plausible explanation by the applicant. Former employers may be able to shed light on the situation or be able to relate the reason given them about gaps by the applicant.

Circumstances relating to termination of previous employment should be clearly related by former employers. Resolve any inconsistencies or vagueness.

Ask former employers as well as the applicant, whether the employee was ever bonded, or was ever refused bonding. Sensitive screening should not result in violating an applicant's civil rights, while assuring you (and your bonding company) that prudent concern is exercised in the hiring process.

B. Bonding

Bonding is also known as fidelity insurance and comes in all configurations; the broader the coverage, the more expensive the premium. One of the most important things you can do is analyze the extent and conditions of coverage in relation to possible misappropriations of funds. Liability is invariably limited in some respects. For example, coverage often does not extend to external fraud; to losses not proven to have been caused by fraudulent acts by covered employees; to frauds committed by employees known to have perpetrated dishonest acts previously; to frauds whose circumstances are not properly investigated; or to frauds whose alleged perpetrators are not brought to trial. Inherent in the analysis of bonding is risk analysis of fraud in relation to specific components to develop a worst-case fraud scenario in terms of dollar-loss before recovery through bonding.

C. Separation of Duties

Separate duties so that no one employee can defraud the company unaided. This is the cardinal rule for fraud prevention, one that is well-understood in manual operations. It is not as well understood in its application to computer processing where a single automated system may combine functions ordinarily separated, such as transactions and adjustments. Analyze all duties, including all stages of computer programming and operations, in terms of defeating single-handed fraud as well as in terms of effectiveness and efficiency, with fraud controls taking precedence. Group review of programmer code before allowing new/upgraded systems into production is the type of duty-separation (function vs. approval) that serves both effectiveness and security.

D. Rotation of Duties

Rotate duties, particularly those involving authorization of a transaction. Separation of duties makes it difficult for an employee to defraud your organization unaided, so that embezzlement becomes a crime of collusion. As more and more embezzlement involves more than one person, it becomes necessary to ensure that the same person is not always involved in approving another's functions. An employee is less likely to initiate a fraudulent transaction if he/she is not certain that his/her accomplice will be the one to approve or process that transaction. Moreover, the knowledge that from time to time other employees will perform his/her function or work his/her cases is a powerful deterrent to any fraudulent scheme, particularly embezzlement which requires continual cover-up.

E. Manual Controls

Manual controls are differentiated from automatic controls because constant review is necessary to see that they are in place and working. Moreover, they often supplement or augment automatic controls; for example, the manual review of claims rejected in computer processing. Review all manual controls to determine the extent to which they would be effective against fraud in any operational area; too often, controls are reviewed without fraud specifically in mind. Classic manual controls are those associated with the tape/disk library, and these controls are strongly associated with restricted access and separation of duties. It does little good to separate programmer/operator duties if the programmer is allowed to sign out production tapes or master files for any reason, especially live-testing. Library controls shall require specific authorization for tape removal for specific periods for specific reasons known to, and sanctioned by, the approving authority. The most important manual controls are those

over blank-check stock and the automatic check-signer. The employee in control of the check-signer shall not at the same time control the check stock, although these duties may be rotated so that the person controlling the check-signer one day may be assigned to control check stock on the following day when a third person is responsible for the check-signer. However, no one individual shall be allowed to “sign” a check he/she has issued. Rotation of duties is proper only for subsequent operations where one's own previous actions have already cleared.

F. Training

Training employees in their responsibilities relative to fraud in their operations is basic to prudent management. This extends beyond the employee's own activities. For example, Title 18, U.S. Code Section 4 requires anyone having knowledge of a Federal crime to report it to the Federal Bureau of Investigation (FBI) or similar authority, with penalties of up to $500 fine and 3 years in jail for failure to do so. No employee should be ignorant of this responsibility. This responsibility can be explained as a simple good citizenship requirement and not spying or snitching. Discuss these things periodically in meetings, along with free give-and-take on moral issues and management's position on every aspect of fraud, including perpetration involving collusion with outsiders. Do not single out any employee or function in these discussions, instead make management's position clear regarding so-called “justification” for unauthorized “borrowing” and the fact that fraud can and will be prosecuted. Explain that there can be no permissive attitude towards dishonest acts because such an attitude is corrupting and makes it difficult for employees to remain honest. Make it known that there are controls throughout the organization to prevent and detect fraud, without being specific as to how they work. Require employees to report apparent loopholes in security that might one day (or already) be exploited for fraudulent purposes. Remind employees that ethical conduct requires their full cooperation in the event of any fraud investigation, and when interviewed they shall be called upon to explain why security gaps or suspicious activities were not reported to the SSO. No security program can be effective without the involvement and cooperation of employees, and nowhere is this truer than with fraudulent activity.

G. Notices

Notices, both periodic and situational, are effective and necessary in the prevention and control of fraud. It is not enough to formulate management policy or to conduct employee training relative to fraudulent activity. It is possible to remind employees of management's continuing concerns and to evaluate employee awareness through simple reminders or announcements of what is happening relative to fraud controls (of a general nature) and management's reliance on their cooperation and understanding of their responsibilities. Without this evidence of sustained management commitment, policy utterances tend to fade from memory or become regarded as part of a new employee's orientation and not part of the scene. This is true of minor abuses, but is also true of abuses that escalate into fraud.

H. Automatic Controls

Automatic controls to prevent or detect fraudulent activities comprise the first line of defense in computer operations. Such controls are often thought of as ensuring data integrity but more in terms of accuracy than of honesty. Evaluate automatic controls in terms of preventing payment to unauthorized persons. Test automatic controls with fraudulent (invalid) input, under strict control of courses, and with management's full cognizance and prior approval.

I. Audit Routines

Audit routines are those programs where trained auditors test for fraud using special routines to reveal computer processing that creates or diverts payments to employees or their accomplices. Wrongdoers not only have to create bogus payments, but also they have to be able to lay their hands on the checks in order to cash them. Devise audit routines to single-out payments being

directed to post office boxes or to repeat addresses (where such repeats would be unreasonable), to the addresses of an employee or his family, or to a drop-off address that is not a real business but merely a place to collect mail.

3 Checklist for Medicare Fraud

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

This checklist represents questions to address in analyzing the security of Medicare fiscal operations.

1) Have Medicare operations been identified where fraud or complicity in fraud may be possible, e.g. initiation/approval of payments?

2) Have individuals been assigned fraud-protection responsibilities in such components, including the responsibility for reporting possible fraud and vulnerability to fraud?

3) Do individual employees at all levels understand that management policy relative to fraud is dismissal and prosecution?

4) Are fiscal operations regularly audited relative to fraud vulnerability?

5) Are fraudulent acts specifically mentioned in the employee's code of ethical conduct?

6) Is employee integrity specifically addressed during the hiring process, and do background investigations elicit information that would uncover an applicant's past fraudulent activity with other employers?

7) Are operations set up in such a way as to discourage both individual and collusive fraudulent activity?

8) Are programs/systems tested by authorized individuals with “fraudulent” input?

9) Are audit trails generated that identify employees who create inputs or make adjustments/corrections that would pinpoint responsibility for any fraudulent act?

10) Is there an effective mechanism for detection/prevention of payments being purposely misdirected to employees, relatives, or accomplices?

11) Are new or changed programs specifically reviewed for fraudulent code by those responsible for production-run approval (persons empowered to review changes but not to make changes themselves)?

12) Are controls designed to prevent fraud, especially in those operations where large sums could be embezzled quickly?

13) Are all error-conditions checked for fraud potential?

14) Are balancing operations done creatively so that an embezzler could not hide discrepancies?

15) Are the official activities of all employees, at all levels, subject to independent review by different reviewers (i.e., not always by the same evaluator)?

16) Does management insist on integrity at all levels?

17) Has management announced that employee's work activities will be reviewed (in unspecified ways) for both the fact and appearance of integrity?

18) Do tape/disk library controls in fact prevent tampering with files/programs for fraudulent purposes?

19) Are alternative fraud controls invoked during emergencies?

20) Are suspected frauds investigated promptly and properly and are they thoroughly documented?

21) Are fraud audits conducted both periodically and randomly?

22) Are random samples taken of claims/bill inputs and checked back to their sources?

23) Does the Personnel Department check the applicant's background, employment record, references, and possible criminal record before hiring?

24) Are badges, identification cards/numbers, and passwords promptly issued and rescinded?

25) Is off-hours work supervised, monitored, or otherwise effectively controlled?

26) Are all employees required to take their vacations and are their replacements required to check over the vacationers' past activities?

27) Are the credentials of outsiders, such as consultants and auditors, checked out?

28) Is temporary help bonded, hired from reputable agencies, and their activities restricted to the tasks to be performed? (Same principle applies to employees temporarily borrowed from non-Medicare components.)

29) Are written procedures controlled and restricted to employees currently assigned the relevant duties?

30) Are special fraud controls specified for backup operations?

31) Are incoming checks, including returned checks, handled by two or more individuals in the mailroom and are such teams switched around so that the same people are not always working together?

32) Are blank checks and automatic check-signing equipment strictly controlled with a tamper-proof numbering mechanism?

33) Is procedure/program documentation relative to the payment process treated as highly sensitive data and safeguarded when superseded?

34) Are backup files current and securely stored off-site?

35) Are re-runs checked for the possibility of fraud, especially duplicate payments?

Transmittals Issued for this Chapter

Rev #	Issue Date	Subject	Impl Date	CR#
R12SS	11/15/2013	CMS Business Partners System Security Manual	01/17/2014	8460
R11SS	09/302011	CMS Business Partners System Security Manual	10/31/2011	7328
R10SS	07/17/2009	Business Partners System Security Manual	08/17/2009	6410
R9SS	06/20/2008	CMS Business Partners System Security Manual	07/22/2008	5976
R8SS	04/06/2007	CMS Business Partners System Security Manual	05/01/2007	5500
R7SS	03/17/2006	Self Assessment Process in Appendix A and Core Security Requirements	05/01/2006	4342
R6SS	12/09/2005	Incorporation of JSM Instructions in sections 1 through 3	01/09/2006	4111
R5SSS	12/23/2004	Miscellaneous Changes in sections 1 through 3	02/28/2005	3605
R4SSM	03/05/2004	Update links, expand on security concepts, clarify core security requirements and security activities to be conducted/followed, include due dates for system security activities and minor editorial changes.	04/05/2004	3106
R3SSM	03/28/2003	Miscellaneous corrections and clarifications in 1-5 and Appendices	04/11/2003	2568
R2SSM	02/13/2002	Replacement of Manual	02/13/2002	2015
R1SSM	03/28/2003	Initial Issuance of Manual	01/26/2001	1439

Centers for Medicare & Medicaid Services
Office of Information Technology (OIT)

Information Security and Privacy Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Standard:

CMS Information Security and Privacy
Acceptable Risk Safeguards (ARS)

CMS Acceptable Risk Safeguards (ARS)

Final

Version 3.1

Document Number: CMS_CIO-STD-SEC01-3.1

November 21, 2017

Effective Date/Approval

This Standard becomes effective on the date that CMS's Chief Information Officer (CIO) signs it and remains in effect until it is rescinded, modified, or superseded.

Signature:	/S/ George Hoffmann Acting Chief Information Officer and Acting Director, Office of Information Technology (OIT)	Date of Issuance	11/21/2017

Standard Owner's Review Certification

This document must be reviewed in accordance with the established review schedule located on the CMS website

Signature:	/S/ Emery Csulak CMS Chief Information Security Officer and Senior Official for Privacy	Date of Annual Review:	11/17/2017

Summary of Changes

Version Number	Editor Name	Date	Table Column Heading	Description of Change
3.0	CMS	01/24/2017	Entire document	Major Revision
3.1	CMS	10/12/2017	Entire document	• Reset control baselines to track to NIST SP 800-53r4 and HHS IS2P selections • Added *Non-Mandatory* designation for controls beyond NIST SP 800-53r4 and HHS IS2P • Revised to improve readability and clarify, standardize formatting • Included discussion and examples on control customization • Realigned CMS CIO and System CIO roles • Clarified information available to CCIC in agreed-upon format and timeframe • Corrected typographical errors • Minor updates to references (e.g., changes to OMB memorandums)

This page intentionally blank.

Table of Contents

1. **Introduction** **1**
1.1 Authority 2
1.2 CMS Information Security and Privacy Program 2
1.3 Version Consolidation 3
2. **Purpose** **5**
3. **Scope** **7**
3.1 External Requirements on CMS Systems 7
4. **ARS Structure** **9**
4.1 ARS Family Descriptions 9
4.2 Control Requirements Structure 13
4.2.1 Security and Privacy Controls 13
4.2.2 Control Enhancements 14
4.2.3 Implementation Standards 15
4.2.4 Supplemental Guidance 16
4.2.5 References 16
4.2.6 Related Control Requirements 16
4.2.7 Priority 16
4.2.8 Assurance 17
4.3 Assessment Procedure 17
4.3.1 Assessment Objective 17
4.3.2 Assessment Methods and Objects 18
4.4 CMS Required Controls and Control Enhancements 18
4.5 ARS Appendix B 19
4.6 Authentication and E-Authentication 20
5. **How to Use the CMS ARS with Customization/Tailoring** **21**
5.1 Mandatory and Non-Mandatory Controls and Control Enhancements 22
5.2 How to Customize/Tailor Implementations for Controls and Control Enhancements 23
5.2.1 Recognizing Keywords that Facilitate Customizing 24

Appendix A. References and Resources **A-1**

Appendix B. ARS Controls **B-1**

Appendix C. Acronyms **C-1**

Appendix D. Glossary **D-1**

Appendix E. Omitted and Not-Selected Controls and Control Enhancements **E-1**

Appendix F. Control and Control Enhancement Implementation Customization/Tailoring..... F-1

List of Tables

Table 1: ARS Security Control Family Descriptions..... 9

Table 2: Controls and Control Enhancements Beyond NIST SP 800-53r4..... 18

Table 3: Keyword and Phrases to Identify Tailorable Controls and Control Enhancements 24

Table 4: Example ARS Control/Control Enhancement Implementation Customization F-1

Table 5: Example Identifying Controls and Control Enhancements as Not Applicable to a System Environment.....F-3

1. Introduction

The *Centers for Medicare & Medicaid Services (CMS) Information Security and Privacy Acceptable Risk Safeguards (ARS)* provides guidance to CMS and its contractors as to the minimum acceptable level of required security controls (i.e., the minimum security and privacy control baselines[1], collectively known as the CMS Minimum Security Requirement [CMSR] baselines) that must be implemented by CMS and CMS contractors to protect CMS' information and information systems, including CMS Sensitive Information.[2] The CMSR is based on:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 (NIST SP 800-53r4), *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013
- Federal Risk and Authorization Management Program (FedRAMP)
- Department of Health and Human Services (HHS) *Information Systems Security and Privacy Policy (IS2P)*
- *CMS Information Systems Security and Privacy Policy (CMS IS2P2) CMS-CIO-POL-SEC-2016-0001*
- CMS policies, procedures, and guidance
- Other federal and non-federal guidance resources
- Industry leading information security and privacy practices adopted by CMS.

This document also provides non-mandatory controls and control enhancements that CMS encourages Business Owners to consider. Many of the mandatory and non-mandatory controls are customizable (i.e., tailorable) by the Business Owner.[3] Business Owners must review all controls since all are relevant and should be considered, even if they are not mandatory to implement, because these controls may help to reduce overall risk.

It should be noted that the minimal baseline for cloud deployments is defined within the FedRAMP Reference Guides.[4] Additionally, previous versions of the ARS consisted of multiple appendices. ARS 3.0, and later versions, are organized within a single document.

---

[1] A control baseline is the minimum list of security controls required for safeguarding an IT system based on the organizationally identified needs for confidentiality, integrity, and/or availability. A different baseline exists for each security category defined by NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

[2] This Policy uses the term "CMS Sensitive Information" as defined in the Risk Management Handbook Volume I Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms* (http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VI_10_Terms_Defs_Acronyms.pdf) and subject to Executive Order 13556, *Controlled Unclassified Information* (https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information). This definition includes all data that require protection due to the risk and magnitude of loss or harm, such as Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI).

[3] The ARS provides guidance on customizing (tailoring) controls and enhancements for specific types of missions/business functions, technologies, or environments of operation. Users of the ARS may tailor specific mandatory controls as well as most of the non-mandatory and unselected controls.

[4] Complete documentation on the FedRAMP baselines is available at https://www.fedramp.gov/resources/documents-2016/.

1.1 Authority

The Office of Management and Budget (OMB) designated the Department of Homeland Security (DHS) and NIST as authorities to provide guidance to federal agencies for implementing information security and privacy laws and regulations, including *Federal Information Security Modernization Act of 2014* (FISMA). Other legislation and regulations affecting CMS include the Privacy Act of 1974 ("Privacy Act") and the *Health Insurance Portability and Accountability Act of 1996* (HIPAA). The ARS addresses CMS applicable information security and privacy control requirements arising from federal legislation, mandates, directives, executive orders, and HHS policy by integrating NIST SP 800-53r4, with the HHS IS2P and specific programmatic legislation and CMS regulations. Appendix A provides references to these authoritative sources.

Per HHS IS2P Appendix A Section 10.2, the CMS Chief Information Officer (CIO) designates the Chief Information Security Officer (CISO) as the CMS authority for implementing the CMS-wide information security program. HHS IS2P Appendix A Section 15 designates the Senior Official for Privacy (SOP) as the CMS authority for implementing the CMS-wide privacy program. Through the ARS, the CIO delegates authority and responsibility to specific organizations and officials within CMS to develop and administer defined aspects of the CMS Information Security and Privacy Program as appropriate. All CMS stakeholders must comply with and support the ARS to ensure compliance with federal requirements and programmatic policies, standards, procedures, and information security and privacy controls.

The CMS CISO or SOP must review any waivers or deviations from the CMSR baselines and make appropriate recommendations to the CIO for risk acceptance.

1.2 CMS Information Security and Privacy Program

CMS has an information security and privacy program managed by the Information Security and Privacy Group (ISPG) under the leadership of the CMS CISO/SOP. ISPG is responsible for ensuring the information security and privacy program:

- Defines CMSR baselines that are compliant with authoritative legislation, statute, directives, mandates, ands overarching policies.
- Provides:
    - Cyber Risk Advisor (CRA) and privacy services to Business Owners and Information System Security Officers (ISSOs)
    - An Authority to Operate (ATO) process
    - A Plan of Actions and Milestones (POA&M) process
    - A common set of security and privacy controls (e.g., policy) that can be inherited across CMS (i.e., Office of the Chief Information Security Officer [OCISO] control catalog)
- Overseeing an inheritable (common) control process that facilitates control inheritance from CMS data centers and under FedRAMP deployments.

1.3 Version Consolidation

Previous versions of the ARS consisted of multiple appendices. Each of these appendices provided the requirements for information systems categorized differently under the NIST Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems.* Separate appendices provided the requirements for systems categorized as High, Moderate, and Low. This concept allowed readers to select the applicable appendix based on system security categorization. However, maintaining three separate appendices required CMS in effect to maintain three versions of the ARS. ARS 3.0, and later versions, identify the controls required for systems categorized under each of the FIPS 199 security categories, and identify controls and control enhancements appropriate for systems that contain Personally Identifiable Information (PII), that contain Protected Health Information (PHI), or are Cloud Service Providers (CSPs)[5]. These later versions of ARS, however, are organized to provide these controls within a single document.

[5] While CSPs are required to comply with FedRAMP baselines, CMS has customized a few of the controls and implementation standards to ensure CMS's assurance requirements are met within a FedRAMP environment.

This page intentionally blank.

2. Purpose

The goal of the ARS is to define a baseline of minimum information security and privacy assurance controls (i.e., the CMSR baselines). These controls are based on both internal CMS governance documents and laws, regulations, and other authorities created by institutions external to CMS.

Protecting and ensuring the confidentiality, integrity, and availability (CIA) for all of CMS' information and information systems is the primary purpose of the information security and privacy assurance program. The ARS complies with the CMS IS2P2[6] by providing a defense-in-depth security structure along with a least-privilege, need-to-know basis for all information access.

Incorporating controls cataloged in the ARS will ensure that CMS and CMS contractor systems meet a minimum level of information security and privacy assurance. CMS systems are also subject to technical security protections defined under CMS' other governance documents (e.g., the *CMS Technical Reference Architecture (TRA),* applicable TRA Supplements, and the *CMS Expedited Life Cycle* (XLC)). These documents, managed under the Office of the CMS CIO, describe architecture and lifecycle standards required of CMS systems.[7]

The controls within the ARS are not intended to be an all-inclusive list of information security and privacy requirements nor are they intended to replace a Business Owner's due diligence to incorporate additional controls to mitigate risk. The ARS controls are the minimum-security and privacy requirements to be considered and employed where applicable throughout the risk management process and the CMS XLC.[8]

[6] The CMS IS2P2 can be found at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

[7] Business Owners may refer to http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html for a complete set of CMS information system development architecture, design, and lifecycle requirements.

[8] Business Owners must review both the non-mandatory (CMS recommended) controls and enhancements listed in the ARS and controls and enhancements under NIST SP 800-53 that were not selected (i.e., those that CMS did not pre-select for inclusion into the ARS as mandatory controls and enhancements, or that CMS selected for inclusion in the ARS but only as non-mandatory controls and enhancements) to determine if any of the controls and/or enhancements would assist in reducing risks to the system.

This page intentionally blank.

3. Scope

All CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions and performing work on behalf of CMS must observe the baseline policy statements described in the *CMS IS2P2*. The ARS controls provide a roadmap to compliance with the *CMS IS2P2* and serve as a guideline to be used throughout the XLC to ensure that CMS information systems are adequately secured and CMS information is appropriately protected.

The Business Owner, assisted by the System Developer/Maintainer, has primary responsibility for evaluating the ARS and determining the appropriateness of each control for their system and ensuring their proper implementation and effectiveness.

3.1 External Requirements on CMS Systems

CMS presumes there are other authorities, both internal and external to CMS, that impose requirements on at least some information systems and business processes. It is the responsibility of the Business Owners of CMS systems, with direction provided by the Office of Information Technology (OIT), to ensure that all applicable internal/external information security and privacy assurance controls are incorporated into CMS systems. Business Owners must document and certify the incorporated controls in their respective system security plan and identify residual risks in the corresponding risk assessment for their system.[9]

For example, any system that receives, processes, or stores, and any devices that transmit, Federal Tax Information (FTI), in addition to complying with ARS, 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.

[9] Residual risk is the risk remaining after efforts have been made to mitigate or eliminate the risk. A residual risk may be known but is not completely controllable (i.e., not fully mitigated), or, it may be unknown. A residual risk is assumed by the Business Owner as the risk for providing the capability/service.

This page intentionally blank.

4. ARS Structure

The information security and privacy controls have a well-defined organization and structure. They are organized into 26 control families for ease of use in the control selection and specification process. The families are established by NIST SP 800-53r4 and are in alignment with the 18 security-related areas specified in FIPS 200,[10] *Minimum Security Requirements for Federal Information and Information Systems*, and the 8 privacy families listed in Appendix J of NIST SP 800-53r4.

The minimal baseline for cloud deployments is defined within the FedRAMP Reference Guides and is not repeated within this document. Complete documentation on the FedRAMP baselines is available at https://www.fedramp.gov/resources/documents-2016/.

4.1 ARS Family Descriptions

Each family contains controls related to the security (or privacy) functionality of the family. A two-character identifier is assigned to uniquely identify each of the security and privacy control families. Table 1 summarizes the 26 control families and the associated two-character identifier used in the ARS.

Table 1: ARS Security Control Family Descriptions

Family (and Identifier)	Description
Access Control (AC)	The controls listed in this section focus on how the organization must limit information system access to authorized users, to processes acting on behalf of authorized users, or to devices (including other information systems); and how the organization must limit the types of transactions and functions that authorized users are permitted to conduct.
Awareness and Training (AT)	The controls listed in this section focus on how the organization must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned IS-related duties and responsibilities.

[10] Of the eighteen security control families in NIST Special Publication 800-53r4, 17 families are described in the security control catalog in Appendix F, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS Publication 200. One additional family (Program Management [PM] family) provides controls for information security programs required by FISMA. This family, while not specifically referenced in FIPS Publication 200, provides security controls at the organization level rather than the information system level.

Family (and Identifier)	Description
Audit and Accountability (AU)	The controls listed in this section focus on how the organization must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Security Assessment and Authorization (CA)	The controls listed in this section focus on how the organization must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Configuration Management (CM)	The controls listed in this section focus on how the organization must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.
Contingency Planning (CP)	The controls listed in this section focus on how the organization must establish, maintain, and implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Identification and Authentication (IA)	The controls listed in this section focus on how the organization must (i) identify information system users, processes acting on behalf of users, or devices; and (ii) authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Incident Response (IR)	The controls listed in this section focus on how the organization must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
Maintenance (MA)	The controls listed in this section focus on how the organization must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Media Protection (MP)	The controls listed in this section focus on how the organization must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Family (and Identifier)	Description
Physical and Environmental Protection (PE)	The controls listed in this section focus on how the organization must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
Planning (PL)	The controls listed in this section focus on how the organization must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
Personnel Security (PS)	The controls listed in this section focus on how the organization must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
Risk Assessment (RA)	The controls listed in this section focus on how the organization must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
System and Services Acquisition (SA)	The controls listed in this section focus on how the organization must: (i) allocate sufficient resources to protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security and privacy assurance considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
System and Communications Protection (SC)	The controls listed in this section focus on how the organization must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security and privacy assurance within organizational information systems.
System and Information Integrity (SI)	The controls listed in this section focus on how the organization must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories, and take appropriate actions in response.

Family (and Identifier)	Description
Program Management (PM)	The PM family provides controls for information security programs required by FISMA. This family, while not specifically referenced in FIPS 200, provides security controls at the organization level rather than the information system level.
Authority and Purpose (AP)	This family assists with Privacy Act compliance by ensuring that organizations: (i) identify the legal bases that authorize a specific collection of PII or activity that impacts privacy; and (ii) specify the purpose(s) for which they collect PII in their notices.
Accountability, Audit, and Risk Management (AR)	This family is intended to enhance public confidence through effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that an organization is complying with all applicable privacy protection requirements and minimizing its overall privacy risk.
Data Quality and Integrity (DI)	This family supports compliance with Section 552a (e)(2) of the Privacy Act of 1974 and enhances public confidence that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.
Data Minimization and Retention (DM)	This family assists organizations in implementing the data minimization and retention elements of the Privacy Act, which require organizations to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. This family also requires organizations to retain PII for only if necessary to fulfill the specified purpose(s) of collecting the PII and in accordance with a NARA-approved record retention schedule.
Individual Participation and Redress (IP)	This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII, as required by the Privacy Act and other laws, regulations, and authorities. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.
Security (SE)	This family supplements security controls to ensure administrative, technical, and physical measures are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that organizational planning and responses to privacy incidents comply with Office of Management and Budget (OMB) policies and guidance. The controls in this family are implemented in coordination with information security personnel using the existing NIST Risk Management Framework.
Transparency (TR)	This family implements Sections 552a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act, which require public notice of an organization's information practices and the privacy impact of government programs and activities.
Use Limitation (UL)	This family is intended to assist organizations in complying with the Privacy Act, which prohibits uses of PII that are either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Implementation of the Controls in this Family will ensure that the scope of PII use is limited accordingly.

4.2 Control Requirements Structure

The CMS-tailored information security and privacy controls include and encompass the NIST, HHS, and IS2P control baselines and serve as the starting point for organizations in determining the appropriate controls and countermeasures necessary to protect their information systems. Many of the CMSR baseline controls may be customized (tailored) to the needs of specific missions, business, information system operations, and operating environments is described in Section 5.

The term *organization* is used throughout the control requirements and associated elements. NIST SP 800-53r4 defines an *organization as: "…an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements)*". CMS extends and clarifies this to include applicable supporting organizations (that is, "…*operational elements*")—including contractor organizations. When assigning minimum roles and responsibilities within control requirements, text may refer to organizational leaders such as the *CIO*. For the purposes of control requirements, these terms are to be interpreted as follows:

- For roles preceded by the term CMS, such as …*approved by the CMS CIO*…; these roles and responsibilities are to be interpreted to refer to the CMS agency official that holds that role or title. In this case, the CMS CIO is the *CIO for the Centers for Medicare & Medicaid Services*.
- For roles not preceded by the term CMS, such as …*approved by the CIO*…; these roles and responsibilities are to be interpreted to refer to the local official that holds that equivalent role or title. In the case of a contractor organization, the CIO might refer to a corporate *Chief Information Officer, Chief Technology Officer, or Director of Information Technology for Medicare Programs*. The "CIO" must be understood to be whatever corporate/organizational role is the equivalent of the "Chief Information Officer" within the applicable organizational structure and scope. Within the CMS government organizational structure, "CIO" will always refer to the CMS CIO.

4.2.1 Security and Privacy Controls

A security or privacy control is the concise statement specifying specific activities or actions needed to protect an aspect of the CMS information or information system at the applicable system security level. Controls are mandatory when defined under the CMSR baseline associated with each FIPS 199 security categorization. However, security or privacy controls may be selected by the Business Owner to strengthen the level of protection provided if deemed appropriate to mitigate or reduce risk.

Security or privacy controls within the ARS are identified by security control family identifier and convey CMS policy, which are based on *minimum* federal requirements, and:

- Employ, and correlate directly to, NIST SP 800-53r4 numbering (e.g., AC-1, AC-2, …).

- Use CMS designators for additional requirements where a direct NIST correlation is not made (e.g., AC-CMS-1).
- Are ordered such that the CMS designators model the NIST designators. The CMS designator numbering restarts at 1 (e.g. AC-1, AC-2, …, AC-CMS-1, AC-CMS-2, …).

NOTE: NIST SP 800-53r4 Appendix J Privacy controls are the exception to the rule above. CMS added an equivalent "dash-1" control for each privacy control family to begin each control family with the policy requirement (e.g., AR-CMS-1).

Each security or privacy control section includes the following:

- *Control Requirement*
  - *Implementation Standards (may not exist for all controls)*
  - *Supplemental Guidance (may not exist for all controls)*
- *References*
- *Related Control Requirements*
- *Assessment Procedure*
  - *Assessment Objectives*
  - *Assessment Methods and Objects*

Each of the above sections of each security or privacy control may contain, in this order: a general statement; a statement concerning systems that contain PII; a statement concerning systems that contain PHI; and a statement concerning systems that are CSPs. Not all controls will contain all statements.

4.2.2 Control Enhancements

Control enhancements supplement controls to achieve the overall required level of protection in accordance with the system security level. *Control enhancements* are mandatory when defined under the CMSR baseline associated with each FIPS 199 security categorization. However, control enhancements may be selected by the Business Owner to strengthen the level of protection provided if deemed appropriate to mitigate or reduce risk.

The control enhancements are structured the same as the base controls, following the same security control family identifier and correlating directly to NIST SP 800-53 (e.g. AC-2(1), AC-2(2), AC-2(3)). Each control enhancement includes the following:

- *Control Requirement*
  - *Implementation Standards (may not exist for all control enhancements)*
  - *Guidance (may not exist for all control enhancements)*
- *References*
- *Related Control Requirements*
- *Assessment Procedure*
  - *Assessment Objectives*
  - *Assessment Methods and Objects*

Each of the above sections of each control enhancement may contain, in this order: a general statement; a statement concerning systems that contain PII; a statement concerning systems that contain PHI; and a statement concerning systems that are CSPs. Not all control enhancements will contain all statements.

4.2.3 Implementation Standards

When an implementation standard is indicated, it is associated with a security or privacy control or control enhancement. The purpose of the implementation standard is to provide a common standard for implementation across CMS for the associated control or control enhancement.

Some standards may contain specific CMS definitions or event values (such as "90 days") to be implemented as the compliance standard for a given control or control enhancement. Other implementation standards are based on specific types of data such as PHI and PII. Finally, implementation standards may be based on specific environments such as CSP implementations.

All implementation standards, whether associated with the control, control enhancement, PII, PHI, or CSP, must be implemented at the designated system security level associated with CMS information and information systems. If a control or control enhancement is mandatory under the CMSR baselines, the implementation standards are mandatory. If a System/Business Owner implements a non-mandatory control or control enhancement, any associated implementation standard defines the minimum implementation.

Risk Management Handbook Volume I Chapter 10 *CMS Risk Management Terms, Definitions, and Acronyms* provide definitions for PII and PHI. Organizations responsible for these types of information must provide the additional safeguards as defined in the implementation standards.

As described above, each control or control enhancement begins with the control requirement, the statement indicating the condition or action necessary to comply with the control. In some cases, the control requirement may include statements indicating how the control requirement may be met if the system contains information of a certain type or processes information a certain way. In the current version of the ARS, these additional statements may be included if the system contains PII; if the system contains PHI; or if the system is maintained by a cloud service provider (to provide cloud services).

After the control requirement statements, the ARS may also include implementation standards. An implementation standard is an additional explanation or action that may be necessary to meet the control requirement for some systems. As for the control requirement statements, implementation standards may be included if the system contains information of a certain type or processes information a certain way. They may also provide parameters for implementing the control requirement. The distinction between control requirements and standards is, the implementation standards may require additional actions (or at minimum, additional knowledge) to that necessary to address to control requirement alone.

4.2.4 Supplemental Guidance

The ARS may include additional *Guidance* to explain the intent of the control or control enhancement. Information within Supplemental Guidance may refer to NIST and other federal publications for further guidance. It is a recommended security practice to refer to the guidance and procedures for additional information to have a clearer and more detailed understanding of specifics of the requirement to assist the organization meeting the CMS security requirements.

4.2.5 References

The references section identifies the section or paragraph designations of the federal source documents which are the basis for the applicable control requirements.

4.2.6 Related Control Requirements

Many, but not all, controls and control enhancements may be *related* to one or more other controls and control enhancements. Additionally, the related controls and control enhancements may provide additional safeguards that can be leveraged to better meet requirements. When addressing some controls, it may be important that their implementation documentation during an assessment or audit be consistent with one or more *related* controls. At the very least, organizations must take care to ensure that related control implementations do not conflict. While every effort was made to identify related controls, other unidentified relationships may exist that are unique to a system, contract type, technology, or organization. Related controls also serve as potential compensating controls and should be used accordingly.

4.2.7 Priority

The priority value listed on the right side of the control or control enhancement title provides the recommended priority codes used for sequencing decisions during security and privacy control implementation. Organizations can use the priority code designation associated with each security and privacy control to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control, a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control, and a Priority Code 0 [P0] indicates the control is not selected for any baseline or has been withdrawn). This recommended sequencing prioritization helps to ensure that the foundational security and privacy controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until all the controls in the system security plan have been implemented. The priority codes are intended only for implementation sequencing, not for making security and privacy control selection decisions.

4.2.8 Assurance

Two fundamental components affecting the trustworthiness of information systems are *security functionality* and *security assurance*. Security functionality is typically defined in terms of the security features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate. Security assurance is the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system—thus possessing the capability to accurately mediate and enforce established security policies. Security controls address both security functionality and security assurance. Some controls focus primarily on security functionality (e.g., PE-3, *Physical Access Control*; IA-2, *Identification and Authentication*; SC-13, *Cryptographic Protection*; AC-2, *Account Management*). Other controls focus primarily on security assurance (e.g., CA-2, *Security Assessment*; SA-17, *Developer Security Architecture and Design*; CM-3, *Configuration Change Control*). Finally, certain security controls can support security functionality and assurance (e.g., RA-5, *Vulnerability Scanning*; SC-3, *Security Function Isolation*; AC-25, *Reference Monitor*). Security controls related to functionality are combined to develop a security capability with the assurance-related controls implemented to provide a degree of confidence in the capability within the organizational risk tolerance.

The ARS specifies assurance-related controls with an "A" in the controls header to identify the security controls that have assurance-related characteristics or properties (i.e., assurance-related controls). Assurance-related controls are discussed in greater detail in NIST SP 800-53r4, Appendix E, *Assurance and Trustworthiness*, to include the allocation of such controls to CMSR baselines. There is no summary table provided in NIST SP 800-53r4 Appendix E for the *Program Management (PM)* family or the *Privacy* families.

4.3 Assessment Procedure

The *Assessment Procedures*, including *Assessment Objectives*, and *Assessment Methods and Objects*, help determine if the security and privacy control implementations in the information system are effective (i.e., implemented correctly, operating as intended, and producing the desired outcome). They provide a foundation to support the security and privacy assessment and authorization process. The "*Assessment Procedure*" section consists of two sub-sections that are designated to achieve one or more objectives by applying methods to assessment objects.

4.3.1 Assessment Objective

The Privacy "*Assessment Objectives*" include a set of *determination statements* ("*Determine if…*") related to the control under assessment. The determination statements are closely linked to the content of the control (i.e., control functionality) to ensure traceability of assessment results back to the fundamental control requirements.

Assessment Objectives for the 26 control families are under development for future versions of the ARS to establish additional expectations for security and privacy control assessments based on the assurance requirements defined in the control. The assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of control effectiveness. Each of the *Assessment Objective determination statements* is either traceable to requirements within the control or control enhancement. This ensures that all aspects of the control are fully assessed and that any weaknesses or deficiencies in the control can be identified and corrective actions taken (usually in the form of a POA&M).

4.3.2 Assessment Methods and Objects

The assessment methods provide a recommended assessment action for evaluators to test the control such as *Examine*, *Interview*, and *Test*. The satisfactory/non-satisfactory result(s) ascertained by the evaluation of the control provides an understanding of the effective implementation of the control. A Risk Posture may be obtained, and/or Risk Based Decisions can be made by combining multiple control evaluation results together.

4.4 CMS Required Controls and Control Enhancements

Ten security and privacy controls and control enhancements are mandatory within the ARS that are not part of the NIST-defined security baselines (i.e., under NIST SP 800-53r4's Appendix D). CMS requires these controls and control enhancements to comply with requirements established by the HHS IS2P or other authorities. Table 2 provides a list of the controls and control enhancements that CMS has added to the NIST-defined security baselines.

Table 2: Controls and Control Enhancements Beyond NIST SP 800-53r4

Control / Control Enhancement	Security Categories	Justification
AC-17(9) (Remote Access | Disconnect/Disable Access)	All	Selected for CMS to support CIO/CISO/SOP orders to disconnect interconnections.
CA-2(3) (Security Assessments | External Organizations)	High	Selected by HHS IS2P.
CA-8 (Penetration Testing)	Moderate	Selected for High Value Asset systems per OMB M-17-09.
IA-2(11) (Identification and Authentication (Organizational Users) | (Remote Access - Separate Device)	Low	Selected for CMS to ensure multifactor authentication meets or exceeds CMS minimal requirements.
MA-4(1) (Nonlocal Maintenance | Auditing and Review)	Moderate, High	Selected by HHS IS2P
MP-CMS-1 (Media Related Records)	All	Selected for CMS to support tracking of media.

Control / Control Enhancement	Security Categories	Justification
SA-15(9) (Development Process, Standards, and Tools | Use of Live Data)	Moderate, High	Selected for CMS to disallow use of production data outside production without prior CMS CIO approval.
SC-15(1) (Collaborative Computing Devices | Physical Disconnect)	All	Selected for CMS to support CIO/CISO/SOP orders to disconnect interconnections.
SC-CMS-1 (Electronic Mail)	Moderate, High	Selected for CMS to ensure electronic mail is processed in accordance with CMS and HHS policy.
SC-CMS-2 (Website Usage)	All	Selected for CMS to facilitate compliance with OMB directives on public facing websites.

4.5 ARS Appendix B

The security and privacy controls within the ARS reflect the requirements established for each CMS System Security Level defined under FIPS 199. When applicable, additional instructions are provided within the control, implementation standard, or supplemental guidance to address situations where privacy information (PII and PHI) is present, or when the system is a CSP.

Each Business Owner is required to determine their system's security level per NIST SP 800-60 *Guide for Mapping Types of Information and Information Systems to Security Categories*, and record the selected information types in CMS Federal Information Security Management Act Controls Tracking System (CFACTS) to ensure the appropriate requirements from FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* are selected.

When a control or control enhancement is mandatory under a given FIPS 199 Security Categorization, the security categorization (i.e., High, Moderate, and Low) is listed within the control header (shaded in blue) and control enhancement header (shaded in green). If a control or control enhancement is non-mandatory under all three security categorizations, the phrase Non-Mandatory is included within the control or control enhancement header (shaded in purple). Each control and control enhancement includes the following additional information:

- Control text defining the requirement (control and control enhancement)
- Additional CMS or data-type specific standards (e.g., CMS defined parameters) that the control must meet (Implementation Standards)
- Additional guidance for clarifying the control (Supplemental Guidance[11])
- The specific laws, standards, or mandates from which the control originated (Authoritative References)
- References to related CMS Policy (CMS IS2P2 clauses)
- Related control requirements

[11] Supplemental Guidance is information provided by NIST and/or CMS to help a reader understand the control or enhancement and implementation standards. The guidance **IS NOT** part of the control or control enhancement and **SHOULD NOT** be thought of as part of the requirement.

- Description of what to test to confirm the control meets its stated purpose (Assessment Objective)
- Recommended objects and methodologies for assessing compliance with each control. (Assessment Methods and Objects)

Privacy and CSP instructions are included within the applicable section (e.g., control, implementation standard, and supplemental guidance) under each control.[12] While each control contains a significant amount of associated information, it should be noted that this information is provided to the user to maximize understanding of the controls themselves; the expectations for reaching compliance with the controls; and the methodologies that will be used to verify compliance.

To assist in identifying mandatory controls or control enhancements, CMS has published a quick reference guide entitled *Quick Reference Guide for the CMS Required Baseline Controls from HHS IS2P, NIST SP 800-53 Rev.4 & FedRAMP*. The guide is available from the CMS Information Security and Privacy Group (ISPG) website at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html or by sending a request to mailto:ciso@cms.hhs.gov.

4.6 Authentication and E-Authentication

Authentication and E-Authentication, formerly an appendix within previous versions of the ARS, has been relocated to the CMS Risk Management Handbook (RMH).

The ARS control IA-2 from the Identification and Authentication control family is the foundation for organizational user authentication requirements. IA-8 is the foundation for non-organizational user authentication requirements. Included with the control are the control enhancements establishing the minimum authentication control requirements. The specific implementation of local and remote authentication and e-Authentication requirements are described in *RMH, Volume III, Standard 3.1, CMS Authentication Standards.*

[12] When additional instructions apply to a control or enhancement, a header has been inserted before the applicable section/text within the Control, Enhancement, Implementation Standards, and/or Guidance section. Additionally, some requirements only apply within specific implementation scenarios.

5. How to Use the CMS ARS with Customization/Tailoring

The security and privacy controls and control enhancements are broadly designed for applicability to the entire CMS organization. Following Section 3 of NIST SP 800-53r4, the process is:

- Categorize the system using FIPS 199 (i.e., High, Moderate, or Low).
- Select the control baseline and determine applicability of controls within the baseline.
- Identify inheritable common security and privacy controls (e.g., through the data center and the OCISO inheritable control catalog).
- Customize/tailor controls as appropriate by adding, providing compensation for controls that cannot be met, and defining parameters/values/attributes. Ensure the implemented controls and control enhancements are effective within your environment.

CMS recognizes that some programs are subject to authorities, both internal and external to CMS, that impose additional requirements on information systems and business processes. Controls and control enhancements that are not listed within the CMSR baselines may be selected and implemented as needed by individual systems to meet these requirements.[13] Additionally, Business Owners must review all controls since all are relevant and should be considered, even if they are not mandatory to implement, because these controls may help to reduce overall risk.

Where applicable, additional instructions are included within the control, implementation standard, or supplemental guidance, for systems that contain individually identifiable information (PII and PHI) or that are CSPs.

A Business Owner may choose to strengthen the control beyond the minimum requirement defined within the ARS to provide the best possible protection of CMS' information and information systems.[14] In some cases, a Business Owner may not need to directly implement some specific controls if they can adequately demonstrate (i.e., show the implementation is effective within their environment) and document that the requirement is satisfied by a parent system (inherited).

[13] It is the responsibility of the Business Owners of CMS systems, with direction provided by OIT, to ensure that all applicable internal/external information security and privacy assurance controls are incorporated into CMS systems.

[14] For example, a system may be required to meet information protection requirements that are more stringent as mandated than the ARS under specific federal, legal, program, or accounting mandates. The ARS control *AU 11 Audit Retention* states that for all systems "The organization retains audit records for ninety (90) days and archives old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory (e.g., Federal Rules of Evidence) and CMS information retention requirements." However, the *National Archives and Records Administration* (NARA) has determined that "Documents relating to periodic audits of teaching facilities nationwide by carriers to recover overpayment" (NC1-440-78-1, Item B) must be retained for four (4) years after completion of an audit. Therefore, if these logs were used as part of such an audit, the NARA requirements would take precedence. The CMS system must therefore be developed to meet these higher-level standards where applicable. The ARS must not be construed to relieve or waive these other standards.

Sometimes Business Owners will be unable to implement information security and privacy controls, even at a minimum level, due to design, resource issues such as funding restrictions, personnel constraints, or hardware/software/facility limitations. Under these circumstances, Business Owners may use compensating controls[15] to reduce the risk to CMS' information, information systems, assets, and reputation. Business Owners must consider implementation of compensating controls as part of a risk-based decision process. These decisions must go through the risk acceptance and risk management processes as a part of the CMS security assessment and authorization (SA&A) program.

The compensating controls must be documented in the system security plan (SSP), and any remaining risk must be documented in accordance with current risk assessment procedure within the information security risk assessment (ISRA), and approved by the Authorizing Official (AO) (i.e., the CMS CIO) or his/her designated representative) using appropriate policy waiver mechanisms.

Any security and privacy control and control enhancement customization must be documented within the SSP to address the system's mission and operational environment. For example, the migration of data into a FedRAMP-approved CSP may require the unique application of specific controls or control enhancements.[16]

The content included in the remainder of this document, including additional information on tailoring, provides a detailed resource for understanding all aspects of the CMS-selected information security and privacy controls. Information on tailoring is also available within NIST SP 800-53r4.

5.1 Mandatory and Non-Mandatory Controls and Control Enhancements

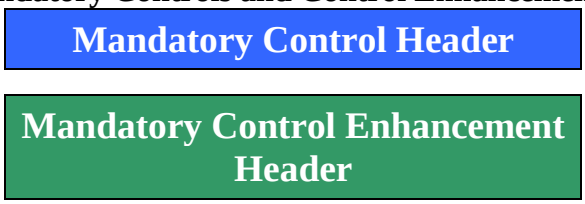
The ARS categorizes the information security and privacy controls and control enhancements as follows:

Mandatory — Controls and control enhancements that are mandatory are identified by a blue (security and privacy control) or green (control enhancement) header. The text within the header identifies the FIPS 199 security category where the control or control enhancement is mandatory. Mandatory controls and control enhancements are included within the CMSR baselines.

[15] Compensating controls are alternative security controls employed by organizations in lieu of specific controls in the low, moderate, or high CMSR baselines (i.e., controls that provide equivalent or comparable protection for organizational information systems and the information processed, stored, or transmitted by those systems).

[16] Additionally, requirements that only apply within specific implementation scenarios are also identified.

Header Colors for
Mandatory Controls and Control Enhancements



Non-Mandatory

While not included within the CMSR baselines, non-mandatory controls and control enhancements may offer additional protection that should be considered by the Business Owner as part of risk management. Non-Mandatory controls and control enhancements are identified as non-mandatory within the (purple) header and apply to all FIPS 199 security categories.[17]

Header Color for
Non-Mandatory Controls and Control Enhancements

Omitted

An omitted control is a control, with associated control enhancements, from NIST 800-53r4, that has been deemed discretionary for implementation within CMS or has been withdrawn by NIST. The discretionary controls are typically associated with environments with far more stringent protection needs such as national security. (See Appendix E for a list of omitted controls and control enhancements.)

Not Selected

Controls and control enhancements from NIST 800-53r4, that are associated with *Mandatory* and *Non-Mandatory* controls but are not included within this ARS are identified as *Not Selected* by CMS. While such control enhancements have not been included within the ARS, they do offer additional protections that the Business Owner should consider. A Business Owner can make a risk-based decision to implement these control enhancements. Control enhancements that are selected by the Business Owner must be documented. (See Appendix E for a list of Not-Selected controls and control enhancements.)

5.2 How to Customize/Tailor Implementations for Controls and Control Enhancements

Business Owners may tailor information security and privacy controls (and control enhancements) within the system SSP to modify and align the controls more closely with the

[17] The text within the header also identifies the control or enhancement as non-mandatory.

specific conditions applicable to the FISMA system. (This is often referred to as scoping.) For example, some systems may require more stringent controls because of the demands of the mission or business function they are supporting, distinctive functionalities of the system, or the environment in which the system operates. Other systems may not need to implement a control or control enhancement because the specific security-related activities or actions are not applicable to the system's environment.

Business Owners wishing to tailor information security or privacy controls must:

- Identify the set of controls that would be applicable to that FISMA system;
- Identify which controls they wish to tailor;
- Select and implement alternative or compensating controls[18], when needed;
- Impose stronger or more restrictive parameters on the implementation of controls;
- Assign specific values to organization-defined (i.e., FISMA System) information security and privacy control parameters via explicit assignment and selection statements;
- Supplement baselines with additional security controls and control enhancements in response to mission requirements, security objectives, technology-driven needs, and other considerations.

However, while tailoring implementation may make selected controls and control enhancements more stringent, tailoring may not be used to make the controls and control enhancements identified as part of the CMSR baselines less stringent without appropriate documentation (within the SSP and ISRA) and approval from the Authorizing Official (i.e., the CMS CIO).

System specific customizing (tailoring) of the system implementations within the SSP is reflected within CFACTS. Examples of customizing controls are provided in Appendix F (*Control and Control Enhancement Implementation Customization/Tailoring*).

5.2.1 Recognizing Keywords that Facilitate Customizing

When reviewing the information security and privacy controls, specific keywords and phrases have been used within the ARS to help identify when a control or control enhancement may be customized/tailored. Several of these keywords and phrases are listed within Table 3.

Table 3: Keyword and Phrases to Identify Tailorable Controls and Control Enhancements

Keyword or Phrase	Guidance
Organization	When the term "organization" is used within a control or control enhancement, it applies to the FISMA system as well as CMS. The Business Owner may tailor the control or control enhancement to address missions/business functions, information systems, or environments of operation. If the control or control enhancement is included within a CMSR

[18] Alternative or compensating controls are controls that ensure the same security goals and interests are fully satisfied as those an otherwise-mandatory control. They may only be used when the use of the mandatory control is not feasible because of the demands of the mission or business function they are supporting, distinctive functionalities of the system, or the environment in which the system operates.

Keyword or Phrase	Guidance
	baseline for a given FIPS 199 security categorization, tailoring may not be used to make the control or control enhancement less stringent.
Defined Personnel	The phrase "defined-personnel" is used within a control or control enhancement to identify when one or more individuals (or roles associated with individuals) need to be associated with the control. The Business Owner must review the default list and tailor the list to address system personnel/roles, missions/business functions, information systems, or environments of operation.
Defined in the	The phrase "defined in the" (e.g., defined in the applicable security plan) is used within a control or control enhancement to identify when a list or value needs to be defined within a specific document or resource. The Business Owner must review the default list or item provided after "defined in the," and indicate what source will provide the definition. For example, the Business Owner may see that the periodicity of an activity is "defined in the [system security plan, privacy impact assessment, or other governance document]," determine that it would be appropriate to defined the periodicity in the system security plan, and then verify that the applicable system security plan does in fact provide the relevant periodicity for the action. Where the controls states that quantifiable value, such as a frequency of an action taken, the source document must provide a value that it no less stringent than the value set by the ARS.
Establishes	The term "establishes" is used within a control or control enhancement to identify when triggers, conditions, and attributes are associated with the control or control enhancement. The Business Owner reviews the default triggers, conditions, and attributes and tailor the triggers, conditions, and attributes to address missions/business functions, information systems, or environments of operation. For example, the Business Owner may see a process associated with an activity must be established. The Business Owner ensures the process is defined and followed as part of the business practices. Triggers, conditions, and attributes that are changed must not be less stringent than the default timeframe.
No Less (or More) Often, At Least	The phrases "no less often", "no more often", and "at least" are used within a control or control enhancement to identify a cycle timeframe. The Business Owner is encouraged to review the default timeframes and tailor the timeframes to address the needs of their system's mission or business function, information system operations, or environment of operation. Timeframes that are changed must not be less stringent than the default timeframe.
Organization(ally)-defined	The phrases "organization-defined" and "organizationally-defined" are used within a control or control enhancement to identify parameter, timeframes, or metric values. The Business Owner is encouraged to review the default values and tailor the values to address the needs of their system's mission or business function, information system operations, or environment of operation. Values that are changed must not be less stringent than the default value. If a default value has not been defined, the Business Owner may define the values as appropriate.
Define, Identify and Select	The terms "define", "identify", and "select" (or variations thereof) are used within a control or control enhancement to indicate that one or more associated "subjects" must be defined and listed. The Business Owner is encouraged to review the default subjects listed and tailor the list to address the needs of their system's mission or business function, information system operations, or environment of operation. Lists that are changed must not be less stringent than the default list.

Keyword or Phrase	Guidance
Parameter Values	All parameter values may be made more stringent. The Business Owner is encouraged to review the default values and tailor the values to address the needs of their system's mission or business function, information system operations, or environment of operation. When changed, parameter values must not be less stringent than the default value. If a default value has not been defined, the Business Owner may define the parameter values as appropriate.

Reviewers are reminded that tailoring to make the controls and control enhancements identified as part of the CMSR baselines less stringent is not permitted without appropriate documentation and CMS approval.

Under some controls and control enhancements, protocols, attributes, and values are limited to provide required interoperability with the CMS Cybersecurity Integration Center (CCIC). Contact your CRA for more information in these cases.

Appendix A. References and Resources

The CMS information security and privacy assurance program and ARS were developed in accordance with Federal mandates and CMS requirements for the handling and processing of CMS' information and information systems. A list of applicable laws across the program is provided below:

A.1 References and Resources

1	Public Law 74-271, Social Security Act, as amended http://www.ssa.gov/OP_Home/ssact/ssact.htm
2	Public Law 93-579, The Privacy Act of 1974, as amended http://www.justice.gov/opcl/privstat.htm
3	Public Law 104-13, Paperwork Reduction Act of 1995, as amended http://www.fws.gov/policy/library/rgpl104-13.pdf
4	Public Law 108–173, Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA), SEC. 912: Requirements for Information Security for Medicare Administrative Contractors http://www.gpo.gov/fdsys/pkg/BILLS-108hr1enr/pdf/BILLS-108hr1enr.pdf
5	Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability https://www.gpo.gov/fdsys/pkg/CFR-2012-title5-vol2/pdf/CFR-2012-title5-vol2-part731.pdf
6	United States Code Title 44 Chapter 33—Disposal of Records http://www.archives.gov/about/laws/disposal-of-records.html
7	GAO-09-232G, Federal Information System Controls Audit Manual (FISCAM), February 2, 2009 http://www.gao.gov/new.items/d09232g.pdf
8	OMB Circulars can be found at the CMS website or at: https://www.whitehouse.gov/omb/information-for-agencies/circulars
9	OMB Memoranda can be found at the CMS website or at: https://www.whitehouse.gov/omb/information-for-agencies/memoranda
10	Homeland Security Presidential Directives can be found at: https://www.dhs.gov/presidential-directives
11	Executive Orders can be found at: http://www.archives.gov/federal-register/executive-orders/disposition.html
12	A list of NIST special publications and FIPS publications can be found at: http://csrc.nist.gov/publications/

13 Additional information on the Federal Risk and Authorization Management Program (FedRAMP) program is found at:
https://www.fedramp.gov/

Documentation on the FedRAMP security and privacy control baselines is available at https://www.fedramp.gov/resources/documents-2016/.

14 The Federal Rules of Evidence can be found at this website:
http://www.uscourts.gov/file/rules-evidence

15 The most recent Internal Revenue Service publication 1075 can be found at:
http://www.irs.gov/pub/irs-pdf/p1075.pdf

16 HHS-OCIO Policy for Information Systems Security and Privacy, dated July 30, 2014 (Send email to FISMA@HHS.gov for a copy)
http://www.hhs.gov/ocio/policy/index.html#Security

17 Additional CMS documents were used as references in the development of this manual. The CMS information security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/ provides a list of applicable CMS documents across the information assurance program.

Appendix B.

B.1 Access Control (AC)

AC-1	Access Control Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates (as necessary) the current:

1. Access control policy at least every three (3) years; and
2. Access control procedures at least every three (3) years.

Implementation Standards:

Systems processing, storing, or transmitting PHI:

PHI.1 - The organization develops, disseminates, and reviews/updates the access control policies and procedures complying with the HIPAA Minimum Necessary Rule and permitted or required uses and disclosures, to limit unnecessary or inappropriate access to PHI.

Supplemental 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 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Access Control policies and procedures form the foundation that allows privacy protections to be implemented for the identified uses of personally identifiable information (PII) and protected health information (PHI). Privacy requirements commonly use the terms “adequate security” and “confidentiality” when referring to access controls and other security safeguards for PII. Applied together, these terms signify the need to make risk-based decisions based on the magnitude of harm (to both organizations and individuals) when determining applicable restrictions for PII. For this overlay, refer to the definitions of “adequate security” in OMB Circular A-130, Appendix III, and “confidentiality” in NIST SP 800-37, Rev. 1, Appendix B. These definitions are consistent with Committee for National Security Systems Instruction (CNSSI) No. 4009.

Reference(s): Code: 5 United States Code (U.S.C.) §552a(b), (e)(9)-(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.514(d)(1)- (5); NIST SP: 800-12, 800-37 Rev. 1 Appendix B, 800-100, 800-122; OMB Memo: M-06-16, M-17-12, Att. 4; OMB Circular A-130: 7.g. and Appendix III	**Related Controls Requirement(s):** PM-9, AR-4, AR-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy and procedures; system security plan, other relevant documents or records.
Examine: Verify that the access control procedures are consistent with access control policy.
Examine: Verify that the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated access control controls.
Examine: Examine document transmission logs or audit logs or records to confirm that the access control policy and procedures have been disseminated or otherwise made available.
Examine: Examine policy and procedure documents to verify that responsible personnel are required to review the access control policy and procedures within the required timeframe and to update as necessary. Examine document changes, document revision records, after-action reports, etc., to ensure reviews were conducted.
Interview: Organizational personnel with access control responsibilities. Verify that personnel:
1. Confirm their respective roles with Access Control policy;
2. Know of and understand Access Control policy and procedures; and
3. Are responsible for reviewing and updating Access Control policy and procedures no less often than required.

AC-2	Account Management (High, Moderate, Low)	P1

Control:

The organization:
a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by defined personnel or roles (defined in the applicable security plan) for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with Acceptable Risk Safeguards (ARS) requirements and Risk Management Handbook (RMH) standards and procedures;
g. Monitors the use of information system accounts;
h. Notifies account managers:
1. When accounts are no longer required;
2. When users are terminated or transferred; and
3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements at least every 90 days for High and Moderate systems or 365 days for Low systems; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Remove or disable default user accounts. Rename active default accounts.
Std.2 - Implement centralized control of user access administrator functions.
Std.3 - Regulate the access provided to contractors and define security requirements for contractors.
Std.4 - Automated account management results must be searchable by the CMS Cybersecurity Integration Center (CCIC):
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Account management information sources include systems, appliances, devices, services, and applications (including databases); and
(c) CCIC-directed account management information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.5 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.
Std.6 - Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.

Systems processing, storing, or transmitting PII (to include PHI):

High:

PRIV.1 - Prohibit use of guest, anonymous, and shared accounts for providing access to PII.
PRIV.2 - Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.
PRIV.3 - Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user's duties.
PRIV.4 - Implement access controls within the information system based on users' or user group's need for access to PII in the performance of their duties.
PRIV.5 - Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties.
PRIV.6 - Create, enable, modify, disable, and remove information system accounts in accordance with the requirement for each user to complete privacy training every 365 days, otherwise the account would be disabled

Moderate:

PRIV.1 - Prohibit use of guest, anonymous, and shared accounts for providing access to PII.
PRIV.2 - Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.
PRIV.3 - Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user's duties.
PRIV.4 - Implement access controls within the information system based on users' or user group's need for access to PII in the performance of their duties.
PRIV.5 - Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties.
PRIV.6 - Create, enable, modify, disable, and remove information system accounts in accordance with the requirement for each user to complete privacy training every 365 days, otherwise the account would be disabled.

Supplemental 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 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 CISO) 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 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.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC

upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Guidance for systems processing, storing, or transmitting PII (to include PHI)

Account management is a critical function for developing and implementing an access control framework that is appropriate for the information contained in systems and applications. When implemented effectively, the access control framework provides the necessary constructs for controlling access to PII, limiting disclosure of records about individuals to only those system and application users that have a need for the information to perform their job functions. The purpose of this guidance is to establish requirements for user access to PHI and PII.

Guidance for systems processing, storing, or transmitting PHI:

The identification of authorized users and access privileges include considerations of whether the user will need access to PHI and whether such access may be permitted or required under HIPAA. The purpose of this guidance is to establish requirements for user access to PHI. Organizations should establish procedures for obtaining necessary electronic protected health information, to include during an emergency.

Reference(s): Code: 5 U.S.C. §552a(b), (e)(9)-(10); FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; HIPAA: 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.502; OMB Memo: M-17-12 Att. 1, M-16-04;	**Related Controls Requirement(s):** AC-3, AC-4, AC-5, AC-6, AC-10, AC-16, 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

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing account management (including creating, enabling, modifying, reviewing, disabling, and removing accounts); system security plan; 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; lists 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; system-generated records with user IDs and last login date; other relevant documents or records.
Examine and Confirm:
1. The organization requires proper identification for all requests for information system access accounts; and
2. Account managers are notified when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes.

Examine: Information system demonstrates that policy is being implemented. Ensure:
1. Only authorized and necessary accounts are enabled;
2. Defined groups consist of only authorized users;
3. Non-interactive system accounts are locked down;
4. Access to privileged accounts is restricted to authorized users; and
5. Information system accounts are reviewed for compliance no less often than required.

Interview: Organizational personnel with account management responsibilities. Ensure personnel know:
1. Access Control policy and procedures;
2. Responsibilities associated with account management;
3. Procedure/process for monitoring the use of guest/anonymous and temporary account; and
4. Organization must remove, disable, or otherwise secure unnecessary accounts.

Test: Test an agreed-upon sample of mechanisms implementing account management functions to confirm that a comprehensive account management process is implemented to verify that only authorized users can gain access to workstations/laptops, applications and networks and the mechanisms are operating as intended and documented. View each “type” of account as documented in the system documentation by doing the following for each type of account:
1. Obtain an account on the system. This will demonstrate that a paper/review/decision process is in place to establish an account;
2. Access the account before it is activated. This should fail;
3. Access the account after its activation. This should pass;
4. Determine whether the password/authenticator was delivered in a secure manner;

5. Test (or have demonstrated) change in account privilege, change to group membership, change to authenticator (usually a password and it may not be on the system, for example, the password protecting a key store in a browser), and disabling (when possible); and
6. Test (or have demonstrated) the termination of an account. This includes assurance that proper record management is undertaken and completed.

AC-2(1)	Automated Information System Account Management (High, Moderate)	P1

Control:

The organization employs automated mechanisms to support the management of information system accounts.

Supplemental Guidance:

The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated, transferred, or change their role; using the information system to monitor account usage; and using telephonic notification to report atypical information system account usage.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System security plan; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system demonstrates automated mechanisms are used to support the management of information system accounts.
Test: Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanisms.

AC-2(2)	Removal of Temporary/Emergency Accounts (High, Moderate)	P1

Control:

The information system automatically disables emergency accounts within 24 hours; and temporary accounts with a fixed duration not to exceed 30 days for High systems and 60 days for Moderate systems.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the information system automatically terminates temporary and emergency account types after no more than ninety (90) days.

Supplemental Guidance:

This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period has elapsed, rather than at the convenience of the systems administrator.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the cloud service provider (CSP) control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System security plan; information system design documentation; information system configuration settings and associated documentation; information system- generated list of active accounts; information system audit records; and other relevant documents or records.
Examine: Information system demonstrates automated mechanisms are used to automatically disable temporary accounts and emergency accounts in defined period. **Test:** Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanism.

AC-2(3)	Disable Inactive Accounts (High, Moderate)	P1

Control:

The information system automatically disables inactive accounts within 30 days for High Systems or 60 days for Moderate Systems.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Procedures addressing account management; system security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; and other relevant documents or records.
Examine: Information system demonstrates automated mechanisms are used to automatically disable inactive accounts in defined period
Test: Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanism.

AC-2(4)	Automated Audit Actions (High, Moderate)	P1

Control:

The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies defined personnel or roles (defined in the applicable security plan).

Implementation Standards:

High & Moderate:

Std.1 - Automated account management audit action results are made available to the CCIC:
(a) Information must be searchable by the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Account management information sources include systems, appliances, devices, services, and applications (including databases).
Std.2 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Supplemental Guidance:

Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):** AU-2, AU-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System security plan; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system demonstrates enabled automated mechanisms that capture audit data on the defined account management actions. For example, verify that the system is configured to capture account creation, account modification, account enabling, account disabling, and account removal actions.
Test: Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanism.

AC-2(5)	Inactivity Logout (High)	P1

Control:

The organization requires that users log out when the time-period of inactivity exceeds 90 minutes and at the end of the user's normal work period.

Supplemental Guidance:

This control enhancement is behavior/policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):** SC-23

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Procedures addressing account management; system security plan; information system design documentation; information system configuration settings and associated documentation; security violation reports; information system audit records; and other relevant documents or records.

Examine: Information system demonstrates enabled automated mechanisms that regulate automated log-out for inactivity and enforcement of work-day access restrictions. Inspect organizational personnel workstations after hours to verify users have logged out.
Interview: Organizational personnel with account management responsibilities.
Test: Automated mechanisms implementing inactivity and work-day time restrictions.

AC-2(11)	Usage Conditions (High)	P1

Control:

The information system enforces organizationally-defined usage conditions and/or circumstances (as defined in the applicable security plan) for organizationally-defined information system accounts.

Supplemental Guidance:

Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.

Reference(s): OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; and other relevant documents or records.
Examine: Verify information system enforces organizationally-defined usage conditions.
Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers. Ensure personnel know system usage limitations.
Test: Ensure automated mechanisms implement account management functions (i.e., usage restrictions are enabled and working).

AC-2(12)	Account Monitoring/Atypical Usage (High)	P1

Control:

The organization:
a. Monitors information system accounts for atypical use; and
b. Reports atypical usage of information system accounts to defined personnel or roles (defined in the applicable security plan), and if necessary, incident response team.

Supplemental Guidance:

Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):** CA-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Procedures addressing account management; system security plan; documentation defining typical/normal use; information system configuration settings and associated documentation; information system audit records; audit tracking and monitoring reports; and other relevant documents or records.
Examine: Information system implements functionality that assists in the detection of atypical use (change in behavior, unusual behavior, etc.) conditions. Examine audit logs or notification trail. Review notifications to specified personnel about user behavior.
Interview: Organizational personnel with account management responsibilities, or information security responsibilities.
Test: Automated mechanisms implementing account management functions. Examine audit logs or notification trail.

AC-2(13)	Disable Accounts for High-Risk Individuals (High)	P1

Control:

The organization disables accounts of users posing a significant risk immediately, not to exceed 30 minutes after discovery of the risk. If this control is selected for systems other than High, a 60-minute window should be used.

Supplemental Guidance:

Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between AOs, information system administrators, and HR managers is essential for timely execution of this control enhancement.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Disabling accounts for high-risk individuals is a minimum requirement for the organization's rules of behavior because of abusing access privileges to sensitive information, including information protected under the Privacy Act of 1974.

Reference(s): Code: 5 U.S.C. §552a(e)(9)-(10); OMB Memo: M-17-12, M-16-04; 45 C.F.R. §164.308(a)(1)(ii)(B); 45 C.F.R. §164.308(a)(1)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(C)	**Related Controls Requirement(s):** PS-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Procedures addressing account management; system security plan; information system configuration settings and associated documentation; information system audit records; audit tracking and monitoring reports; and other relevant documents or records.
Examine: Information system implements functionality that assists in disabling accounts if a user (or system account) is found to pose an unacceptable risk. Review notifications to specified personnel about user risk.
Interview: Organizational personnel with account management responsibilities, or information security responsibilities.
Test: Automated mechanisms implementing account management functions. Verify account is disabled within required timeframe following simulated user risk assessment.

AC-3	Access Enforcement (High, Moderate, Low)	P1

Control:

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Systems processing, storing, or transmitting PII (to include PHI):

The organization controls access to PII through access enforcement mechanisms.

Implementation Standards:

High, Moderate, & Low:

Std.1. If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13).
Std.2. Configure operating system controls to disable public "read" and "write" access to all system-related files, objects, and directories as well as files, objects, and directories that contain sensitive information.
Std.3. Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas.

Supplemental 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, 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 RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.
Well-designed, automated access controls (e.g., mandatory access control [MAC], discretionary access control [DAC], role-based access control [RBAC], or attribute-based access control [ABAC]) limit user access to information per defined access policies, which helps ensure the security and confidentiality of sensitive information contained in the system.
FIPS 140-2 validation certificate numbers are listed at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Well-designed, automated access controls (e.g., MAC, DAC, RBAC, or ABAC limit user access to information per defined access policies, which helps ensure the security and confidentiality of the sensitive information, such as PII and PHI, contained in the system.
For example, implement role-based access controls and configure access controls so that each user can access only the pieces of information necessary for the user's role or only permit users to access PII through an application that restricts their access to the PII the users require, instead of allowing users direct access to a database or files containing PII.

Reference(s): Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; FISCAM: AC-3, AS-2; HIPAA: 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(a)(2)(ii), 45 C.F.R. §164.312(a)(2)(iv); OMB Memo: M-06-16	**Related Controls Requirement(s):** AC-2, AC-4, AC-5, AC-6, AC-16, 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

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing access enforcement; system security plan; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; if cryptography is implemented, FIPS 140-2 validation certificate number(s); other relevant documents or records. The access control procedures should specify the process for obtaining authorization as a requirement prior to gaining access to the information system. **Examine:** Information system implements functionality that enforces access controls. Examples:
- RBACs
- DACs
- MACs
- usage limitations
- connection limitations
- restrictions to functions with elevated privileges
- restrictions to critical system functions (e.g., boot functions/basic input output system [BIOS])

Examine: Examine the information system access control configuration parameters (e.g., access control lists [ACL], file permissions, group definitions, and user profiles), including a review of file systems and data management systems to verify that they are configured in accordance with access control policy and procedures.
Test: Automated mechanisms implementing access enforcement functions. Test a sample of system mechanisms that implement access control to confirm that the mechanisms are operating in accordance with policy and procedures.
This control applies to applications with an integrated access control mechanism, such as WinZip and SecureZip, as well as the underlying operating system. These applications must meet CMS requirements (FIPS 140-2 validated module).

AC-4	Information Flow Enforcement (High, Moderate)	P1

Control:

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Implementation Standards:

High & Moderate:

Std.1 - The CMS CIO, CISO, and SOP have the authority to order the immediate termination and/or suspension of any interconnection that, in the judgment of the CMS officer and CMS Security Operations, present an unacceptable level of risk to the CMS enterprise and/or mission.

Supplemental Guidance:

Information flow control regulates where information can travel within an information system and between information systems (as opposed to who can 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); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regarding mechanisms to reassign security attributes and security labels.
Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. NIST SP 800-53 control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross- domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial-off-the-shelf (COTS) information technology products.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The information flow enforcement controls provide a technical means of implementing disclosure requirements by minimizing information shared between networks, devices, and individuals within information systems and between interconnected systems. This control can also limit information transfers between organizations based on data structures and content.

Reference(s): Code: 5 U.S.C. §552a(b); FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b); NIST SP: 800-47; OMB Memo: M-06-19, M-17-12 Web: ucdmo.gov	**Related Controls Requirement(s):** AC-3, AC-16, AC-17, AC- 19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; 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; other relevant documents or records. Ensure that the system documentation describes:
1. The process for ensuring that each user receives only authorized information;
2. How the system processes all data traversing the network interface per the applied access policy and/or filtering mechanism; and
3. Any requirements of boundary defense mechanisms at layered or internal enclave boundaries.

Examine: Information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems. Examples:
- RBAC/MAC enabled;
- Networking is configured to enforce intended routing (e.g., disabling proxy/source/ redirect routing, Internet Protocol (IP) spoofing, broadcasting);
- IPv6 is disabled unless explicitly authorized; and
- Firewall rules adhere to a deny-all, permit-by-exception policy.

Examine: Confirm that the system design is capable of enforcing assigned authorizations for controlling the flow of information within the system and between interconnected systems. The system must verify that only data that is explicitly permitted (based on the filtering policies) is released from one network enclave to another network enclave.

Interview: Administration personnel knowledge of information flow and interconnection processes and procedures.
Test: Automated mechanisms implementing information flow enforcement policy and mechanisms. Test a specific sample of the information system automated mechanisms implementing information flow enforcement policy to confirm that the mechanisms are operating as intended. Attempt to send information to improper destinations (systems or users). Verify that the system detects the impermissible flow, prevents it, audits the violation, and notifies the appropriate personnel.

AC-5	Separation of Duties (High, Moderate, Low)	P1

Control:

The organization:
a. Separates duties of individuals as necessary (defined in the applicable security plan), to prevent malicious activity without collusion;
b. Documents separation of duties; and
c. Defines information system access authorizations to support separation of duties.

Systems defined as CSPs:

For CSPs, the information system enforces role-based access control policies over all subjects and objects where the policy specifies that:
a. The policy is uniformly enforced across all subjects and objects within the boundary of the information system; and
b. A subject that has been granted access to information is constrained from doing any of the following;

1. Passing the information to unauthorized subjects or objects;
2. Granting its privileges to other subjects;
3. Changing one or more security attributes on subjects, objects, the information system, or information system components;
4. Choosing the security attributes and attribute values to be associated with newly created or modified objects; or
5. Changing the rules governing access control.

Implementation Standards:

High:

Std.1 - Audit functions must not be performed by security personnel responsible for administering access control.
Std.2 - Maintain a limited group of administrators with access based upon the users' roles and responsibilities.
Std.3 - The critical mission functions and information system support functions must be divided among separate individuals.
Std.4 - The information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals or groups.
Std.5 - An independent entity, not the Business Owner, ISSO, System Developer(s)/Maintainer(s), or System administrator(s) responsible for the information system, conducts information security testing of the information system.
Std.6 - The quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions must be conducted by an independent entity rather than the code developers.

Moderate:

Std.1 - Audit functions must not be performed by security personnel responsible for administering access control.
Std.2 - Maintain a limited group of administrators with access based upon the users' roles and responsibilities.
Std.3 - The critical mission functions and information system support functions must be divided among separate individuals.
Std.4 - The information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals or groups.
Std.5 - An independent entity, not the Business Owner, ISSO, System Developer(s)/Maintainer(s), or System administrator(s) responsible for the information system, conducts information security testing of the information system.

Low:

Std.1 - Audit functions must not be performed by security personnel responsible for administering access control.
Std.2 - Maintain a limited group of administrators with access based upon the users' roles and responsibilities.
Std.3 - The critical mission functions and information system support functions must be divided among separate individuals.
Std.4 - The information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals or groups.

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization:
a. Assigns user accounts and authenticators in accordance within service provider's role-based access control policies;
b. Configures the information system to request user ID and authenticator prior to system access; and
c. Configures the databases containing federal information in accordance with service provider's security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate.
CSP.2 - FedRAMP-defined subjects may explicitly be granted FedRAMP-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all the above constraints.
CSP.3 - AC-5 is not required at Low level for FedRAMP-authorized CSPs.

Supplemental 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.
Separation of duties aligns privileges with appropriate roles with the idea that duties are split between roles in such a way as to reduce the risk of malevolent or inappropriate behaviors based on access. Implementing this control helps reduce the risk of inappropriate access to sensitive information (e.g., separating employees that perform security investigations from mission and business functions).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Separation of duties aligns privileges with appropriate roles with the idea that duties are split between roles in such a way as to reduce the risk of malevolent or inappropriate behaviors based on access. Implementing this control helps reduce the risk of inappropriate access to PII (e.g., separating employees that perform security investigations from mission and business functions).
Separation of duties is implemented by designating a selected set of administrators the capability to set user permissions to PII and PHI information, while those administrators do not themselves have access to the PII and PHI. The principle of separation of duties is significant for developers as well as for operational system administrators.

Guidance for systems processing, storing, or transmitting PHI:

HIPAA requires the separation of duties to ensure that checks and balances are designed into the system to limit the effect of any given end user to control the entire process. Roles and responsibilities should be divided so that a single end user cannot subvert a critical process. This practice divides the tasks related to maintaining system security among different personnel such that no single individual could compromise PHI.

Reference(s): Code: 5 U.S.C. §552a(e)(9)-(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-4, SD-1, SD-2; HIPAA: 45 C.F.R. §164.308(a)(3)(i), 164.308(a)(4)(i), 45 C.F.R. §164.308(a)(4)(ii)(A), 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(c)(1)	**Related Controls Requirement(s):** AC-3, AC-6, PE-3, PE-4, PS-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing division of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; list of user accounts and privileged accounts; information system audit records; and other relevant documents or records.
Examine: Verify that an access control mechanism resides on the information system that prevents users from having all the necessary authority or information access to perform malicious activity without collusion.
Examine: Examine system configuration files to confirm that access authorizations have been set up properly for the various roles. Confirm that access control mechanism residing on the information system is configured to prevent users from having all the necessary authority or information access to perform malicious activity without collusion. **Examine:** Information system implements functionality that enforces separation of duties. Examples:
- RBACs and schema are defined and used;
- Privileged escalation mechanisms (tools) require authentication; and
- Shared accounts are not used.

Interview: Organizational personnel with responsibilities for defining appropriate division of responsibility and separation of duties. Confirm privileged users have limited duties.
Test: Automated mechanisms implementing separation of duties policy.

Systems defined as CSPs:

(i) Not applicable to FEDRAMP services.
(ii) Evaluate adherence of systems deployed atop of FedRAMP deployments to CMSR basic requirements.

AC-6	Least Privilege (High, Moderate)	P1

Control:

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with CMS missions and business functions.

Implementation Standards:

High & Moderate:

Std.1 - Disable all file system access not explicitly required for system, application, and administrator functionality.
Std.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 CMS security policy.
Std.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.
Std.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.
Std.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.

Low:

Std.1 – When implemented, disable all file system access not explicitly required for system, application, and administrator functionality.
Std.2 – When implemented, 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 CMS security policy.
Std.3 – When implemented, restrict the use of database management utilities to only authorized database administrators.
Std.4 – When implemented, disable all system and removable media boot access unless it is explicitly authorized by the CMS CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected.

Supplemental 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.
The concept of least privilege aligns with the notion of only allowing access to sensitive information when an individual has a need-to-know in performance of their job duties.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The concept of least privilege aligns with the notion of only allowing access to PII when an individual has a need-to-know in performance of their job duties.
The organization enforces the most restrictive set of rights/privileges or access needed by users (or processes acting on behalf of users) for the performance of specified tasks — increasing the level of restriction as PII confidentiality impact level rises.
The organization ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) necessary to perform their assigned tasks.

Guidance for systems processing, storing, or transmitting PHI:

HIPAA requires least privilege to satisfy both the Minimum Necessary Rule and access control safeguards.

Reference(s): Code: 5 U.S.C. §552a(b); FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.502(b), 45 C.F.R. §164.308(a)(4)(ii)(A), 45 C.F.R. §164.312(a)(1); Homeland Security Presidential Directive (HSPD)-7: D(10); OMB Memo: M-06-16;	**Related Controls Requirement(s):** AC-2, AC-3, AC-5, CM-6, CM-7, PL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Confirm that privileged accounts are created for users to perform privileged functions only; that is, privileged users use non-privileged accounts for all non-privileged functions. Review how least privilege is determined for each user. Verify that each of the users has been granted the least privilege for the user's job in accordance with system documentation.
Examine: Information system implements functionality enforcing least privilege functions. Examples:
- RBACs and schema are defined and used;
- Privileged escalation mechanisms (tools) require authentication;
- No orphaned files (files not owned by a known system user) or files with uneven permissions (e.g., world has more access rights than the owner) exist on the system;
- Unexpected files and directories with excessive permissions (e.g., world write);
- Remote mounts/file shares minimize access granted;
- File protections minimize unauthorized access to sensitive files;
- Access by users to functionality is limited to functionality required for role/job;
- Access to privileged applications is limited;
- System accounts minimize access (e.g., not available for interactive use);
- Applications that are not configured to maximize security; and
- Unnecessary accounts have been removed.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. Confirm that the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
Test: Automated mechanisms implementing least privilege functions [this is least functionality—different control]. Inspect system inventory to verify that only required applications are installed. Test a sample of the information system functions, particularly functions that require access for specific tasks by users and privileged users to confirm that the system has been configured with the most restrictive set of rights, privileges, or accesses possible and that users have been assigned the most restrictive set of rights, privileges, or accesses necessary. Verify that least privilege for the user has been assigned to the access of system resources.
The inventory of installed applications for deployed systems can be used to as an input to assess least privilege.

Systems defined as CSPs:

(i) Not applicable to FedRAMP services.
(ii) Evaluate adherence of systems deployed atop of FedRAMP deployments to CMSR basic requirements.

AC-6(1)	Authorize Access to Security Functions (High, Moderate)	P1

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:
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:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.
CSP.2 - For CSPs, the organization defines the list of security functions. The list of functions is approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Limiting access to security functions to authorized personnel reduces the number of users able to perform certain security functions, such as configuring access permissions, setting audit logs, performing system management functions. Examples of authorized personnel include security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. These types of security functions can provide a level of access to PII, and capabilities to manipulate it, in ways that other users' roles typically could not.
The organization identifies the security relevant functions that require authorized access for all information systems that contain moderate or high PII confidentiality impact level information.

Reference(s): Code: 5 U.S.C. §552a(b)(1); FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16; 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.502(b)	**Related Controls Requirement(s):** AC-17, AC-18, AC-19

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing least privilege; list of security functions 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.
Examine: Verify that the organization explicitly authorizes access to the control-specified list of security functions at a minimum (deployed in hardware, software, and firmware) and security-relevant information:
Examine: Information system implements functionality enforcing restrictions on access to security applications. Verify access to defined security functions and security information has been granted to specifically authorized personnel only.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.
Test: Automated mechanisms forcing authorization prior to access to security functions.
The organization may also implement a solution that forces a user to go through an additional authorization before access to an elevated privilege is granted to security applications. (This may include privilege elevation applications such as sudo or the use of multiple accounts for users with access to elevated privileges.)

Systems defined as CSPs:

(i) Not applicable to FEDRAMP services.
(ii) Evaluate systems deployed atop of FedRAMP deployments adhere to CMSR basic requirements.

AC-6(2)	Non-Privileged Access for non-security Functions (High, Moderate)	P1

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, audits 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:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization requires that users of information system accounts, or roles, with access to all security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

Supplemental 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 RBAC 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control requires system users with elevated privileges to use their non-privileged accounts when performing non-security functions. Requiring system users to use their non-privileged accounts when working with PII for purposes other than security functions limits inadvertent access to or disclosure of PII and protects the integrity of PII. Any access involving PII that is non-administrative in nature should require the user to use their non-privileged accounts to perform that function.

Reference(s): Code: 5 U.S.C. §552a(b); FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16; 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.502(b)	**Related Controls Requirement(s):** PL-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; 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.
Examine: Information system implements functionality enforcing use of non-privileged accounts/roles before being granted access to applications with elevated privileges. Confirm that procedures exist limiting performance of privileged functions to privileged accounts only, and that all non-privileged activities are relegated to non-privileged accounts. Verify that individual privileged users also have a non-privileged account.
Examine: Examine the information system security configuration files and user accounts with parameters including assigned privileges to confirm that privileged accounts have been created for privileged users to perform privileged functions. Review the listing of privileged system user accounts. Identify the user accounts that have system privileges (e.g., system users who have the capability to perform system functions including change system configuration, reset security policy and settings, start/shut down system, perform system backup, data restore). Confirm that access to privileged accounts is limited to privileged users. Review detailed configuration and analyze for indications to the contrary that privileged accounts are created and used only for privileged functions.
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.
Test: Automated mechanisms implementing least privilege functions. Confirm that security functions and security-relevant information cannot be accessed from a non-privileged account.

AC-6(3)	Network Access to Privileged Commands (High)	P1

Control:

The organization authorizes network access to privileged commands only for compelling operational needs as defined in the System Security Plan and documents the rationale for the information system.

Supplemental Guidance:

Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Examples include:
- Setting/modifying audit logs and auditing behavior;
- Setting/modifying boundary protection system rules;
- Configuring/modifying access authorizations (i.e., permissions, privileges);
- Setting/modifying authentication parameters; and
- Setting/modifying system configurations and parameters.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This controls restricts network access (i.e., access across a network connection as opposed to local access, such as being physically present at a device to access) to perform privileged commands.

Reference(s): Code: 5 U.S.C. §552a(b)(1); OMB Memo: M-06-16	**Related Controls Requirement(s):** AC-17

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing least privilege; list of privileged commands assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system implements functionality restricting network access to privileged commands to only documented accounts/roles. Confirm that procedures exist limiting network-based performance of privileged functions to documented accounts/roles only. Confirm that the applicable security plan documents a compelling operational need for any network-based privileged access.
Examine: Examine the information system security configuration files and user accounts. Identify the user accounts that are allowed network-based access to privileged commands. For each identified account, confirm that network-based access to privileged commands is documented in the applicable security plan.
Interview: Organizational personnel with responsibilities for assigning network access to privileged commands.
Interview: Organizational personnel granted network access to privileged commands.
Test: Automated mechanisms implementing least privilege functions. Confirm that security functions and security-relevant information cannot be accessed from a non-privileged account.

AC-6(5)	Privileged Accounts (High, Moderate)	P1

Control:

The organization restricts privileged accounts on the information system to personnel or roles (as defined in the security plan).

Supplemental Guidance:

Privileged accounts, including super user accounts, are typically described as system administrator for various types of COTS 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control limits who is authorized to administrative accounts, such as those who can perform security functions, which include configuring access permissions, setting audit logs and performing system management functions. These types of system and network management personnel typically have a level of access that is capable of circumventing other access controls. Limiting access to these accounts further protects sensitive information by limiting the number of individuals that have the “keys to the kingdom” on a network or system.

Reference(s): Code: 5 U.S.C. §552a(b)(1); FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16; 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.312(a)(1)	**Related Controls Requirement(s):** CM-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing least privilege; list of system-generated super user accounts; list of system administration personnel; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Privileged accounts/roles on information systems are restricted to defined personnel. Examine configuration files to verify that access to privileged accounts has been granted to only organization-defined personnel.
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.
Test: Automated mechanisms implementing least privilege functions. Automated mechanisms ensure only accounts with appropriate privileges can access privileged function.

AC-6(7)	Non-Mandatory: Review of User Privileges	P3

Control:

The organization:
a. Reviews the privileges assigned to defined personnel or roles defined in the applicable security plan every 90 days to validate the need for such privileges; and
b. Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance:

The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Review of user privileges is necessary to ensure privileges are revoked for those who no longer require access to sensitive information. Implementation of this control reduces the risk of unauthorized access to sensitive information by users who no longer need access to perform their job functions.

Reference(s): Code: 5 U.S.C. §552a(b) , (e)(9)-(10); OMB Memo: M-17-12; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.312(a	**Related Controls Requirement(s):** CA-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization:
(i) Reviews the privileges assigned to defined personnel or roles defined in the applicable security plan every 90 days to validate the need for such privileges; and
(ii) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing review of roles and personnel reassignment; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records.
Examine: Information system implements functionality that assists in the periodic review of user privileges. Examine evidence of privileges review, such as meeting records, system change records.
Interview: Organizational personnel with responsibilities for reviewing least privileges necessary to accomplish specified tasks.
Test: Automated mechanisms implementing review of user privileges.

AC-6(9)	Auditing Use of Privileged Functions (High, Moderate)	P1

Control:

The information system audits the execution of privileged functions.

Supplemental 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 (BYOD).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Privileged functions have elevated permissions to access, and grant access, to sensitive information. Accountability requires the ability to detect, trace, and audit a privileged function whenever it is executed.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g. and Appendix III; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R.§164.312(b)	**Related Controls Requirement(s):** AU-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system implements functionality that audits the execution of privileged functions. Examine audit records for evidence of execution of privileged functions.
Test: Automated mechanisms auditing the execution of least privilege functions. Automated mechanisms ensure accessing privileged functions appear in audit trails.

AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions (High, Moderate)	P1

Control:

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental 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 that 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Non-privileged users may not have the same level of trust as privileged users. Privileged functions have access beyond that of the typical user, and as such may have greater ability to access sensitive information. Individual accountability requires the ability to trace (audit) the actions of the user who initiated them.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g. and Appendix III	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing Non-Privileged Users executing Privileged Functions; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system implements functionality that prevents non-privileged users from executing privileged functions. Examine audit records, searching for attempts by non-privileged users to use privileged functions.
Test: Automated mechanisms implementing least privilege functions for non-privileged users. Attempt to access a privileged function from a non-privileged account. Attempt to disable, circumvent and/or alter implemented safeguards/countermeasures. Attempt should fail.

AC-7	Unsuccessful Logon Attempts (High, Moderate, Low)	P2

Control:

The information system:
a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and

b. Automatically disables or locks the account/node until released by an administrator or after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded.

Implementation Standards:

High:

Std.1 - Configure the information system to lock out the user account automatically after three (3) invalid login attempts during a 120-minute time window. Require the lock out to persist until released by an administrator.

Moderate:

Std.1 - Configure the information system to lock out the user account automatically after five (5) invalid login attempts during a 120-minute time window. Require the lock out to persist for a minimum of one (1) hour

Low:

Std.1 - Configure the information system to disable access for at least fifteen (15) minutes after five (5) invalid login attempts during a 120-minute time window.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the information system:

a. Enforces a limit of not more than three (3) consecutive invalid login attempts by a user during a fifteen (15) minute time; and
b. Automatically locks the account/node for thirty (30) minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

Supplemental Guidance:

This control applies regardless of 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 release 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 both the operating system and the application levels.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; OMB M-16-04	**Related Controls Requirement(s):** AC-2, AC-9, AC-14, IA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing unsuccessful login attempts; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system implements functionality that limits number of consecutive invalid login attempts and automatically locks accounts.
Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts. Test to confirm that the information system automatically enforces a limit of OpDiv-defined number of consecutive invalid access/logon attempts by a user at which point the information system automatically locks the user's account or node. Verify that once locked, a user account or node remains locked until a period has elapsed, or the account is released by an authorized administrator or other action occurs.

AC-8	System Use Notification (High, Moderate, Low)	P1

Control:

The information system:
a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner states:
* This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes (1) this computer network, (2) all computers connected to this network, and (3) all devices and storage media attached to this network or to a computer on this network.
* This system is provided for Government authorized use only.
* Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties.
* Personal use of social media and networking sites on this system is limited as to not interfere with official work duties and is subject to monitoring.
* By using this system, you understand and consent to the following:
- The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system.
- Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose
b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems:
1. Displays system use information when appropriate, before granting further access;
2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Includes a description of the authorized uses of the system.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization determines elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Joint Authorization Board (JAB).
CSP.2 - For CSPs, the organization determines how System Use Notification is going to be verified and provides appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB.
CSP.3 - For CSPs, 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. The documented agreement on how to provide verification of the results are approved and accepted by the JAB.

Supplemental Guidance:

The warning banner language has very important legal implications for CMS and its information system resources. Should content need to be added to this banner, submit the modified warning banner language to the CMS CIO for review and approval prior to implementation. If an information system has character limitations related to the warning banner display, the CMS CIO can provide an abbreviated warning banner version. If this banner is inconsistent with any directives, policies, regulations, or standards, notify the CMS CIO immediately.
All information system computers and network devices under CMS control, prominently display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, websites, web pages where substantial personal information from the public is collected, Secure File Transfer Protocol (SFTP), Secure Shell (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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

System use notification (e.g., logon banner) does not satisfy the requirement for Privacy Act Statements or Privacy Act system of records notice, when applicable; see TR-1 and TR-2. System use notifications are the primary, interactive vehicle for notifying system users prior to accessing a system of the organization's monitoring practices and reminding users that unauthorized use is both prohibited and subject to criminal and civil penalties.
The system use notification requires explicit action from the system user to acknowledge the notice before they can enter the system. Notices on system use are principally intended to convey information regarding consent to monitor (and other security-relevant information). These notices may also be, in some instances, an appropriate means to remind system users that the system being accessed contains sensitive PII and requires due care (e.g., a logon banner on an employee management system).

Guidance for systems processing, storing, or transmitting PHI:

Note that System Use Notification does not satisfy the requirement for privacy notice under the HIPAA Privacy Rule.

Reference(s): Code: 5 U.S.C. §552a(e)(3) and (e)(4); FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; Department of Health and Human Services (HHS): Policy for Monitoring Employee Use of HHS IT Resources; OMB Circular A-130: 7.g.; 45 C.F.R. §164.520(1)(i)	**Related Controls Requirement(s):** TR-1, TR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Assessment 1
Examine: Access control policy; privacy and security policies; system security plan; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; and other relevant documents or records.
Examine: Information system implements the required message or banner. All vectors for system access need to be evaluated. These include but are not limited to:
1. Console (text or graphical user interface [GUI] console);
2. Remote access (e.g., Remote Desktop Protocol [RDP], SSH); and
3. Window Manager

Test: Automated mechanisms implementing the access control policy for system use notification. Confirm that the system use notification message remains on the screen until the user takes explicit actions to logon to the information system.
Assessment 2
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 notification messages; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system implements the required banner. All vectors for system access need to be evaluated. This includes:
1. Console (text console)
2. Remote access (e.g., RDP, SSH)
3. Window Manager

Test: Automated mechanisms implementing the access control policy for system use notification. Confirm that the system use notification message remains on the screen for a sufficient time for the user to notice and make a positive acknowledgement.

AC-10 | Concurrent Session Control (High) | P3

Control:

The information system limits the number of concurrent sessions for each system account to one (1) session for both normal and privileged users. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.

Supplemental 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 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing concurrent session control; information system design documentation; information system configuration settings and associated documentation; applicable security plan; and other relevant documents or records.
Examine: Information system implements the required limits on concurrent sessions. Confirm that a requirement (if applicable) for more than one concurrent session is documented in the applicable security plan.
Test: Automated mechanisms implementing the access control policy for concurrent session control. Confirm that the information system limits the number of concurrent sessions for users to the organization-defined number of sessions.

AC-11	Session Lock (High, Moderate)	P3

Control:

The information system:
a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity (for both remote and internal access connections) or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Implementation Standards:

High & Moderate:

Std.1 - Period of inactivity must be no more than 15 minutes before session lock occurs for remote and mobile devices and requires user re-authentication. As agencies continue to migrate to laptops and docking stations making clients increasingly mobile, this is a logical extension of that requirement.

Supplemental 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.
This control protects sensitive information from unauthorized access when system users are away from their workstation. Since 2007, OMB has required session lock for remote and mobile devices, a standard which is neither technically nor financially burdensome. Based on risk, many agencies have adopted 15-minute session locks by policy as a best practice. Remote connections, as defined under AC-17, originate from outside the system boundary. Internal connections originate within the system boundary.
Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control protects personally identifiable information (PII) from unauthorized access when system users are away from their workstation. Since 2007, OMB has required session lock for remote and mobile devices, a standard which is neither technically nor financially burdensome. Based on risk, many agencies have adopted 15-minute session locks by policy as a best practice.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): Code: 5 U.S.C. §552a(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.312(a)(2)(iii); OMB Memo: M-06-16, M-17-12; 45 C.F.R. §164.312(a)(1)	**Related Controls Requirement(s):** AC-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; system security plan; and other relevant documents or records.
Examine: Information system implements the required limits on inactivity functionality.
Test: Automated mechanisms implementing the access control policy for session lock. Confirm that the information system initiates a session lock after the organization-defined period of inactivity and maintains the session lock until the user reestablishes access using established identification and authentication procedures. Confirm user can initiate session lock, and then unlock session using established identification and authentication procedures.

AC-11(1)	Pattern-Hiding Displays (High, Moderate)	P3

Control:

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental 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 conveys sensitive information.

Guidance for systems defined as CSPs:

Publicly viewable images can be easily implemented under Information as a Service (IaaS) and Platform as a Service (PaaS) based environments.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

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; and other relevant documents or records.
Examine: Information system implements inactive session concealment functionality.
Test: Information system session lock mechanisms. Confirm that, when activated, the information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

AC-12	Session Termination (High, Moderate)	P2

Control:

The information system automatically terminates a user session after defined conditions or trigger events (defined in the applicable security plan) requiring session disconnect.

Supplemental 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, time-of-day restrictions on information system use.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The session termination control requires implementing functionality to prevent unauthorized use of an established user session. This control protects sensitive information from unauthorized access when system users have initiated a session.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s):	**Related Controls Requirement(s):** SC-10, SC-23

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; system security plan; and other relevant documents or records.
Examine: Information system automatically terminates a user session after defined conditions or events occur (as defined in the system security plan). Examine the applicable security plan-defined events and functionality that requires session termination.
Test: Automated mechanisms implementing the account control policy for session termination. Confirm defined events cause a session to be terminated.

AC-14	Permitted Actions Without Identification or Authentication (High, Moderate, Low)	P3

Control:

The organization:
a. Identifies specific user actions that can be performed on the information system without identification or authentication;
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication; and
c. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

Supplemental Guidance:

This control addresses situations in which organizations determine that no identification or authentication is required in 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 facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Individual accountability requires the ability to trace (audit) the actions of the user who initiated them when accessing personally identifiable information (PII). Therefore, un-identified and un-authenticated users must not access PII.

Guidance for systems processing, storing, or transmitting PHI:

Individual accountability requires the ability to trace (audit) the actions of the user who initiated them when accessing PHI. Therefore, un- identified and un-authenticated users must not access PHI.

Reference(s): Code: 5 U.S.C. §552a(b); FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; OMB Circular A-130: 7.g. and Appendix III; 45 C.F.R. §164.312(a)(2)(i)	**Related Controls Requirement(s):** AC-2(9), CP-2, IA-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; system security plan; list of information system actions that can be performed without identification and authentication; information system audit records; and other relevant documents or records.
Examine: Information system identifies specific user actions that can be performed on the information system without identification or authentication. Examples:
- Access to files or services without authentication (anonymous access); and
- Anonymous FTP.
Interview: System/network administrators; organizational personnel with information security responsibilities. Confirm that they have followed the guidelines provided and to further confirm that the organization has documented the rationale for providing such access.
Test: Automated mechanisms implementing the policy for user actions not requiring identification and authentication. Confirm that the system is configured to allow for specific actions that a user is permitted to perform without identification and authentication.

AC-17	Remote Access (High, Moderate, Low)	P1

Control:

The organization monitors for unauthorized remote access to the information system (including access to internal networks by VPN). Remote access for privileged functions must be permitted only for compelling operational needs, must be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If remote access is authorized, the organization:
a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.
c. Access to HHS Webmail using personally owned equipment is authorized. Access to other systems/networks using personally-owned equipment is prohibited without written authorization from the CIO, or an approved policy allowing the use of personally-owned equipment:
1. Personally-owned equipment must be scanned before being connected to CMS (and HHS) systems or networks to ensure compliance with CMS requirements; and
2. Personally-owned equipment must be prohibited from processing, accessing, or storing Department sensitive information unless it is approved in writing by the CMS SOP and employs CMS required encryption (FIPS 140-2 validated module).

Implementation Standards:

High, Moderate, & Low:

Std.1 - Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified within every three hundred sixty-five (365) days.
Std.2 - If e-authentication is implemented as a remote access solution or associated with remote access, refer to RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.
Std.3 - All computers and devices, whether government furnished equipment (GFE), contractor furnished equipment (CFE), or personal, that require any network access to a CMS network or system are securely configured and meet, as a minimum, the following security requirements:
(a) Up-to-date system patches;
(b) Current anti-virus software;
(c) Host-based intrusion detection system;
(d) Functionality that provides the capability for automatic execution of code disabled; and
(e) employs CMS required encryption (FIPS 140-2 validated module).
Std.4 - For organizations supporting remote access (including teleworking), ensure NIST SP 800-46 guidelines are followed by defining policies and procedures that define:
(a) Forms of permitted remote access;
(b) Types of devices permissible for remote access;
(c) Type of access remote users are granted; and
(d) How remote user account provisioning is handled.

Supplemental 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 VPNs to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs, does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, 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. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3.
For minimum authentication requirements, refer to RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Limiting access to personally identifiable information (PII) from remote networks and/or restricting activities that can be conducted with PII remotely reduces the risk of intentional and unintentional disclosures of PII that may not exist on an internal network.
Allow remote access to PII only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

Guidance for systems processing, storing, or transmitting PHI:

Implement technical security measures to guard against unauthorized remote access to electronic PHI that is being transmitted over an electronic communications network.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(c); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(e)(1); NIST SP: 800-46, 800-77, 800-113, 800-114, 800-121; OMB Memo: M-06-16, M-17-12	**Related Controls 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

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system implements established and documented usage restrictions:
1. Monitors for unauthorized remote access;
2. Remote access to privileged functions (functions w/elevated privileges) is controlled;
3. Remote access requires authentication; and
4. Applications, to include network protocols, used for remote access are configured to maximize security.
Examine: Information system has been configured to restrict remote access to documented and approved ports and protocols. Examples:
- Only authorized ports and protocols (e.g., SSHv2, Secure Network Management Protocol version 3 [SNMPv3]) are enabled; and
- Encryption enforces use of FIPS 140-2 validated modules and cyphers
Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities.
Test: Remote access management capability for the information system. Examples of conditions that typically violate this control:
- Disallowed (insecure) protocols (e.g., Telnet, SSHv1, SNMPv1/v2, SSL v3.0) enabled;
- Encryption using non-FIPS 140-2-validated cryptographic algorithms or modules;
- Liberal remote access (e.g., any remote user with a valid account);
- Remote applications not configured to maximize security; and
- Remote access protocols not enforcing re-authentication.

AC-17(1)	Automated Monitoring/Control (High, Moderate)	P1

Control:

The information system monitors and controls remote access methods.

Implementation Standards:

High & Moderate:

Std.1 - The organization implements CMS and federally distributed blocking rules within one hour of receipt.

Supplemental Guidance:

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and 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). Auditing remote access ensures unauthorized connections to information systems containing sensitive information can be detected across all information system platforms (e.g., servers, mobile devices, work stations).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Auditing remote access ensures unauthorized connections to information systems containing personally identifiable information (PII) can be detected across all information system platforms (e.g., servers, mobile devices, work stations).
Audit all remote access to, and actions on, resources containing PII.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-06-16, M-17-12, M-14-03, M-15-01, M-16-04; 45 C.F.R. §164.310(b); 45 C.F.R. §164.310(c); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(e)(1)	**Related Controls Requirement(s):** AU-2, AU-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system implements remote access monitoring and control functionality.
Test: Automated mechanisms monitoring and controlling remote access methods.

AC-17(2)	Protection of Confidentiality/Integrity Using Encryption (High, Moderate)	P1

Control:

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Supplemental Guidance:

The encryption strength of a mechanism is selected based on the security categorization of the information. Use only the CMS-approved encryption standard (see SC-13).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Encrypting remote sessions protects the confidentiality and integrity of sensitive information.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16, Step 3; 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(e)(2)(ii);	**Related Controls Requirement(s):** SC-8, SC-12, SC-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
Test: Cryptographic mechanisms protecting confidentiality and integrity of remote access sessions.

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Examine: Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
Test: Cryptographic mechanisms protecting confidentiality and integrity of remote access sessions.

AC-17(3)	Managed Access Control Points (High, Moderate)	P1

Control:

The information system routes all remote accesses through a limited number of managed access control points. The organization must identify acceptable network access control points (e.g., connections standardized through the TIC initiative).

Supplemental Guidance:

Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the TIC initiative requirements for external network connections.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):** SC-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system limits remote access to defined, secure, and managed access points, ports, and protocols.
Interview: System/network administrators; organizational personnel with information security responsibilities.
Test: Automated mechanisms routing all remote accesses through managed network access control points.

AC-17(4)	Privileged Commands/Access (High, Moderate)	P1

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.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AC-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; system security plan; information system audit records; and other relevant documents or records.
Examine: Information system restricts remote access to privileged commands and access to security-relevant information. Examine documented rationale for each user's or group's remote access to execute privileged commands.
Test: Automated mechanisms implementing remote access management. Example: Disabling root access under *NIX sudo command.

AC-17(9)	Disconnect/Disable Access (High, Moderate, Low)	P1

Control:

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within one (1) hour.

Implementation Standards:

High, Moderate, & Low:

Std.1 - The organization terminates or suspends network connections (i.e., a system to system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP).

Systems defined as CSPs:

High & Moderate:

CSP.1 - The organization terminates or suspends network connections with 15 minutes of direction by CMS.

Supplemental Guidance:

This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.
CMS Business Owners are to ensure that required Interconnection Security Agreements (ISA) and Memoranda of Understanding (MOU) are established and that they state the interconnections may be terminated or suspended by CMS unilaterally based solely on CMS' interpretation of the risk.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing connection disconnect; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records.
Examine: Information system provides the ability to disconnect or disable remote access within the required period.
Test: Automated mechanisms implementing remote access management.

AC-18	Wireless Access (High, Moderate, Low)	P1

Control:

The organization monitors for unauthorized wireless access to information systems and prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If wireless access is authorized, the organization:
a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access;
b. Authorizes wireless access to the information system prior to allowing such connections;
c. The organization ensures that:
1.The CMS CIO must approve and distribute the overall wireless plan for his or her respective organization; and
2. Mobile and wireless devices, systems, and networks are not connected to wired HHS/CMS networks except through appropriate controls (e.g., VPN port) or unless specific authorization from HHS/CMS network management has been received.

Implementation Standards:

High, Moderate, & Low:

Std.1 - If wireless access is explicitly approved, 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 stateful inspection firewall is implemented between the wireless network and the wired infrastructure;
(e) MAC address authentication is utilized;
(f) Static IP addresses, not Dynamic Host Configuration Protocol (DHCP), is utilized;
(g) Personal firewalls are utilized on all wireless clients;
(h) File sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall;
(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis;
(k) Adheres to CMS-CIO-POL-INF12-01, CMS Policy for Wireless Client Access; and
(l) Adheres to the HHS Standard for IEEE 802.11 Wireless Local Area Network (WLAN).
Std.2 - Wireless printers and all Bluetooth devices such as keyboards are not allowed.

Supplemental Guidance:

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., Extensible Authentication Protocol/Transport Layer Security [EAP/TLS], Protected Extensible Authentication Protocol [PEAP]), which provide credential protection and mutual authentication.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; HHS: IS2P 2014; NIST SP: 800-48, 800-94, 800-97	**Related Controls Requirement(s):** AC-2, AC-3, AC-17, AC- 19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; and other relevant documents or records.
Examine: Information system/network components monitor for unauthorized access, to include wireless, and detect/report the installation of wireless access points.
1. Use of wireless printers and Bluetooth devices is not allowed without explicit approval by the Authorizing Official (AO).
Interview: Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system.
Test: Wireless access management capability for the information system.
A Network Access Control (NAC) capability is an example of a utility that can be deployed to detect the installation of a wireless access points. The NAC would be configured to deny access by default.

AC-18(1)	Authentication and Encryption (High, Moderate)	P1

Control:

If wireless access is explicitly approved, the information system protects wireless access to the system using encryption, and authentication of both users and devices.

Supplemental Guidance:

Ensuring wireless connections use authentication and encryption reduces the risk that an unauthorized device or user will gain access to the system or intercept communications.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Communication over wireless networks, unless properly secured, has a greater risk of interception than hard-wired networks. Implementing encryption of wireless network communications containing personally identifiable information (PII) renders any intercepted data unreadable.
If wireless networks permit access to organization information systems containing PII, then encryption of content and authentication of users or devices is required. Organizations should ensure that all WLAN components use FIPS-approved cryptographic algorithms to protect the confidentiality and integrity of WLAN communications.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-97, 800-153	**Related Controls Requirement(s):** AC-3, IA-2, IA-3, IA-8, SC- 8, SC-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. **Examine:** Information system protects wireless access to the system using encryption, and authentication of both users and devices. Examine encryption mechanism details to verify that encryption is performed by a FIPS 140-2-validated cryptographic module operating in the FIPS-approved mode of operation.
Interview: Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system.
Test: Wireless access usage and restrictions. Automated mechanisms implementing the access control policy for wireless access to the information system.

AC-18(4)	Restrict Configurations by Users (High)	P1

Control:

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

Supplemental Guidance:

Organizational authorizations to allow selected users to configure wireless networking capability are enforced, in part by the access enforcement mechanisms employed within organizational information systems.

Reference(s):	**Related Controls Requirement(s):** AC-3, SC-15

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. **Examine:** Information system restricts the ability to configure wireless networking to designated users and/or roles.
Interview: System/network administrators; organizational personnel with information security responsibilities.
Test: Automated mechanisms preventing independent configuration of wireless networking capabilities.

AC-18(5)	Antennas/Transmission Power Levels (High)	P1

Control:

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Supplemental Guidance:

Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) Reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations;
(ii) Employing measures such as TEMPEST to control wireless emanations; and
(iii) Using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals.
Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area.

Reference(s):	**Related Controls Requirement(s):** PE-19

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. **Test:** Automated mechanisms implementing the access control policy for wireless access to the information system; Wireless connections and access points outside of organizational boundaries using scanning devices.

AC-19	Access Control for Mobile Devices (High, Moderate, Low)	P1

Control:

The organization:
a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. CIO authorizes the connection of mobile devices to organizational information systems.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Encrypt information on all mobile devices that contains PII.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization defines inspection and preventative measures. The measures are approved and accepted by the Joint Authorization Board (JAB).

Supplemental Guidance:

A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried 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 near the individual; however, the degree of proximity can vary depending upon 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 upon 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 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Limiting access to sensitive information from mobile devices reduces the risk of intentional and unintentional disclosures sensitive information PII that may not exist on an internal network.

Reference(s):	**Related Controls 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-43, SI-3, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system restricts/precludes access to interfaces and ports that support use of mobile devices. **Interview:** Organizational personnel who monitor for unauthorized mobile device connections to CMS information systems. **Interview:** Organizational personnel who use portable and mobile devices to access the information system.
Test: Automated mechanisms monitoring and implementing access control policy for portable and mobile devices.

AC-19(5)	Full Device/Container-Based Encryption (High, Moderate)	P1

Control:

The organization employs CMS-required (FIPS 140-2 validated module) full-device encryption or container encryption to protect the confidentiality and integrity of information on approved mobile devices.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Encrypt information on all mobile devices that contain low, moderate, and high PII confidentiality impact level information.

Supplemental Guidance:

Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including, for example, encrypting selected data structures such as files, records, or fields. FIPS 140-2 approved security function families are found at http://csrc.nist.gov/groups/STM/cavp/validation.html. However, implementing an approved security function is the start. The product must also be on the approved validation lists. (See http://csrc.nist.gov/groups/STM/cmvp/documents/140- 1/140val-all.htm for a list of current validated products.)

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Since mobile devices are more likely to be lost or stolen, sensitive information on a mobile device is more vulnerable. Encryption reduces this vulnerability.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16; 45 C.F.R. §164.312(a)(2)(iv)	**Related Controls Requirement(s):** MP-5, SC-13, SC-28

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing access control for mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Mobile device systems implement CMS required (FIPS 140-2 validated module) functionality that provides full disk encryption or container encryption.
Test: Mechanisms implementing encryption control policy for mobile devices.
Full disk/device encryption applications must be configured to meet CMS requirements (FIPS 140-2 validated module).

AC-20	Use of External Information Systems (High, Moderate, Low)	P1

Control:

The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If external information systems are authorized, the organization establishes strict terms and conditions for their use. The terms and conditions must address, at a minimum:
a. The types of applications that can be accessed from external information systems;
b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
c. How other users of the external information system will be prevented from accessing federal information;
d. The use of VPN and stateful inspection firewall technologies;
e. The use of and protection against the vulnerabilities of wireless technologies;
f. The maintenance of adequate physical security controls;
g. The use of virus and spyware protection software; and
h. How often the security capabilities of installed software are to be updated.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Only organization owned computers and software can be used to process, access, and store PII.
PRIV.2 - Privacy requirements must be addressed in agreements that cover relationships in which external information systems are used to access, process, store, or transmit and manage PII.
PRIV.3 - Access to PII from external information systems (including, but not limited to, personally owned information systems/devices) is limited to those organizations and individuals with a binding agreement to terms and conditions of privacy requirements which protect the PII.

Supplemental 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 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 non-federal governmental organizations; and (iv) federal 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 federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. 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 federal agencies or organizations subordinate to those agencies, 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 regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon 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 (e.g., individuals accessing federal information through www.medicare.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: 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.
For some external systems, those systems operated by other federal agencies, including organizations subordinate to CMS, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Access to PII from external information systems (including, but not limited to, personally owned information systems/devices) is reinforced by a binding agreement to terms and conditions of the organization's privacy requirements to ensure awareness and accountability of both parties.
Such agreements may include memoranda of understanding (MOU), terms of service, or contracts.

Reference(s): Code: 5 U.S.C. §552a(e)(10); FAR: Part 24, 39.105; FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AS-1, SM-7; HHS: IS2P 2014; OMB Circular A-130: 7.g.; 45 C.F.R. §164.312(a)(2)(i)	**Related Controls Requirement(s):** AC-1, AC-3, AC-17, AC- 19, CA-3, PL-4, SA-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) Only organizational owned computers and software are used to process, access, and store PII.

Assessment Methods and Objects:

Examine: Access control policy; system security plan; 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; and 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. **Test:** Where authorized, external information systems connecting to the organization to store, access, transmit, or process sensitive information comply with CMS and organizational requirements.

AC-20(1)	Limits on Authorized Use (High, Moderate)	P1

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.

Supplemental 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), so as not to compromise, damage, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

An external information system which processes, stores, or transmits sensitive information needs to have its security controls verified to meet the organization's security control requirements for information systems processing sensitive information.

Reference(s): Code: 5 U.S.C. §552a(e)(10); FAR: Part 24, 39.105; FedRAMP Rev. 4 Baseline; OMB Circular A- 130: 7.g.; 45 C.F.R. §164.314(a)	**Related Controls Requirement(s):** CA-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing the use of external information systems; system security plan; information system connection or processing agreements; account management documents; and other relevant documents or records.
Examine: Organization implements limitations on use of external information systems for external processing, storage, and transmission of organization-controlled information.
Test: Automated mechanisms implementing limits on use of external information systems.

AC-20(2)	Portable Storage Devices (High, Moderate)	P1

Control:

The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Supplemental 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 the devices may be used and under what conditions the devices may be used.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing the use of external information systems; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records.
Examine: Organization restricts the use of organization-controlled portable storage devices on external information systems to authorized individuals. Examine list of users authorized to use portable storage on documented external information systems.

AC-20(3)	Non-Mandatory: Non-Organizationally Owned Systems/ Components/ Devices	P3

Control:

The organization restricts the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.
a. Use of contractor owned devices must be documented within the contract and the system security plan, employ information security and privacy protections appropriate for the sensitivity of the data, and be approved by the Authorizing Official (AO) in advance; and
b. Use of personally owned devices must comply with HHS and CMS policies and directives on use of personally-owned information systems and components.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - At a minimum, controls must include implementation of either full-device or virtual container encryption to reduce the vulnerability of PII contained on mobile devices.
PRIV.2 - Prior to being provided access to PII on remote devices, device users must acknowledge through a binding agreement their responsibilities to safeguard the PII accessible from the device and that they are aware of and agree to the organization's capabilities to manage the organization's PII on the device, including confiscation, in consultation with the organization's counsel, if necessary to remove the PII.

Supplemental Guidance:

Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies, contractors) and personally owned devices. There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, it may be such that the use of non-organizationally owned devices is allowed but restricted in some way. Restrictions include, for example: (i) requiring the implementation of organization-approved security controls prior to authorizing such connections; (ii) limiting access to certain types of information, services, or applications; (iii) using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and (iv) agreeing to terms and conditions for usage. For personally owned devices, organizations consult with the Office of the General Counsel regarding legal issues associated with using such devices in operational environments, including, for example, requirements for conducting forensic analyses during investigations after an incident.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Mobile devices are more vulnerable to loss or theft than other types of computing media (e.g., desktops and servers) due to their portability and widespread use inside and outside of government facilities. This means PII stored on a mobile device is more vulnerable. This security control implements protections for PII contained on any mobile device not owned by the organization, including personal mobile devices, commonly referred to as BYOD.
The organization should include in its mobile strategy a method to ensure both the device's access to PII can be revoked and the device's PII contents can be remotely removed.

Reference(s): Code: 5 U.S.C. §552a(e)(10); HHS: IS2P 2014; OMB Memo: M-17-12, M-06-16	**Related Controls Requirement(s):** AC-19(5)

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; procedures addressing Bring Your Own Device (BYOD), security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records.
Examine: Information system restricts the use of portable storage devices.
Interview: Organizational personnel with responsibilities for restricting or prohibiting use of non-organizationally owned information systems, system components, or devices; system/network administrators; organizational personnel with information security responsibilities; organizational personnel on use of BYOD.
Test: Automated mechanisms implementing restrictions on the use of non-organizationally owned systems/components/devices.

AC-21	Information Sharing (High, Moderate)	P2

Control:

The organization:
a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required; and
b. Employs defined automated mechanisms, or manual processes, (defined in the applicable security plan) to assist users in making information sharing/collaboration decisions.

Supplemental Guidance:

This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information (PII), classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When PII is shared, it is necessary to ensure the PII is being shared in accordance with statutory and regulatory requirements, including any restrictions on how the PII may be shared and the requirements for security of the receiving partner.
This control addresses the sharing of information in a general sense (i.e., disclosure). It is not "information sharing" as defined by the Information Sharing Environment (ISE) Privacy Guidelines. All sharing partners, processes, and information systems must comply with applicable system of records notices (SORN), Privacy Impact Assessments (PIA), or other forms of notice or public statements. Examples of actions that may be required to implement privacy requirements in information sharing activities include: addressing privacy requirements in information sharing agreements; ensuring sharing partners have a mutual understanding of the PII confidentiality impact level (as NIST SP 800-122 is a risk based analysis and accepts variation in organizational implementation); developing processes and supporting mechanisms to ensure/enforce compliance; and implementing technical capabilities that enforce privacy requirements for PII stored or processed by a sharing partner. Program managers and system owners should work with their privacy offices to ensure information sharing activities are compliant with privacy requirements.

Guidance for systems processing, storing, or transmitting PHI:

The CMS Senior Official for Privacy (SOP) may permit a business associate to create, receive, maintain, or transmit PHI on behalf of the organization to the extent the business associate is required by law to perform such function or activity, without meeting the requirements of a business associate contract, provided that the SOP attempts in good faith to obtain satisfactory assurances required in the business associate contracts, and documents the attempt and the reasons that these assurances cannot be obtained. This control helps covered entities to enforce the Minimum Necessary Rule.

Reference(s): Code: 5 U.S.C. §552a(b) and (e); FedRAMP Rev. 4 Baseline; Privacy: Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment; 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.314(a)	**Related Controls Requirement(s):** AC-3, TR-1, UL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; 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; and other relevant documents or records.
Examine: Information system restricts sharing of identified information to authorized users/roles.
Interview: Organizational personnel responsible for making information sharing/collaboration decisions.
Test: Automated mechanisms or manual process implementing access authorizations supporting information sharing/user collaboration decisions.

AC-22	Publicly Accessible Content (High, Moderate, Low)	P3

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.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization reviews the content on the publicly accessible organizational information system for nonpublic information at least quarterly.

Supplemental Guidance:

In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the 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 public, typically without identification or authentication. The posting of information on non-CMS information systems is covered by organizational policy.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

A system of records maintaining personally identifiable information (PII) that is not approved for release under the Freedom of Information Act (FOIA) is nonpublic information. When agencies consider sharing or posting PII, they must do so in a way that fully protects individual privacy. Under HIPAA, a covered entity or business associate may not use or disclose protected health information except as provided by the HIPAA Privacy Rule. This control implements procedures to protect information, including PII, from being posted publicly improperly.
PII that is nonpublic information must not be posted onto a publicly accessible information system.

Reference(s): Code: 5 U.S.C. §552(b)(6); FedRAMP Rev. 4 Baseline; OMB Memo: M-11-02; 45 C.F.R. §164.502(a)	**Related Controls Requirement(s):** AC-3, AC-4, AT-2, AT-3, AU-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; system security plan; 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.
Examine: Information system restricts sharing of identified information to authorized users/roles.
Interview: Organizational personnel responsible for managing publicly accessible information posted on organizational information systems.
Test: Automated mechanisms implementing management of publicly accessible content.

B.2 Awareness and Training (AT)

AT-1	Security Awareness and Training Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to personnel/roles as designated by the organization:
1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and, if necessary, updates the current:
1. Security awareness and training policy at least once every three (3) years; and
2. Security awareness and training procedures at least once every three (3) years.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Information security awareness and training complements privacy awareness and training efforts, particularly when awareness and training efforts address topics where the two disciplines overlap, such as on topics related to use, confidentiality, access, integrity, and the protection of sensitive information. Coordination between the information security and privacy offices on the proper use and protections to be afforded to personally identifiable information (PII) within security awareness and training policies addresses the purpose, roles and responsibilities surrounding PII compliance.

Reference(s): Code: 5 U.S.C. §552a(e)(9)-(10), Public Law (PL) No. 107-347, §208; Executive Order: 13587; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3, SM-4; HIPAA: 45 C.F.R. §164.308(a)(5)(i), 45 C.F.R. §164.308(a)(5)(ii)(A), 45 C.F.R. §164.308(a)(5)(ii)(B); NIST SP: 800-12, 800-16, 800-50, 800-100; OMB Memo: M-03-22, M-17-12	**Related Controls Requirement(s):** AR-5, AR-6, PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security and privacy awareness and training policy and procedures, personnel training records; and other relevant documents.
Interview: Organizational personnel with information security and privacy awareness and training responsibilities, verify that these individuals are aware of the scope of this requirement.

AT-2	Security Awareness Training (High, Moderate, Low)	Assurance	P1

Control:

The organization provides basic security 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
c. Within every three hundred sixty-five (365) days thereafter.

Implementation Standards:

High, Moderate, & Low:

Std.1 - An information security and privacy education and awareness training program must be developed and implemented for all employees and individuals working on behalf of CMS who access, use, manage, or develop information systems.
Std.2 - Information security and privacy education and awareness training must address individuals' responsibilities associated with sending sensitive information in email. **Std.3 -** Privacy awareness training must be provided before granting access to CMS systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors, to explain the importance of and responsibility for safeguarding PII and ensuring privacy, as established in federal legislation and OMB guidance.

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Provide privacy training for all systems that collect, maintain, store, use, or disclose PII, commensurate with the PII confidentiality impact level. Integrate privacy training with general Information Assurance training.

Supplemental Guidance:

Organizations determine the appropriate content of security and privacy awareness and 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 must provide a basic understanding of the need for information security and privacy; descriptions of user actions necessary to maintain security and privacy and instruction on how to respond to suspected security and privacy incidents. The content must also provide awareness of the need for operations security and privacy as they relate to CMS's information security and privacy program. Security and privacy awareness techniques may 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Information security awareness and training complements privacy awareness and training efforts, particularly when awareness and training efforts address topics where the two disciplines overlap, such as on topics related to use, confidentiality, access, integrity, and the protection of sensitive information.

Guidance for systems processing, storing, or transmitting PHI:

The following elements of security training are addressable under HIPAA. Security Awareness Training should include:
(i) periodic security updates;
(ii) procedures for guarding against, detecting, and reporting malicious software;
(iii) procedures for monitoring log-in attempts and reporting discrepancies; and
(iv) procedures for creating, changing, and safeguarding passwords.

Reference(s): Code: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; Executive Order: 13587; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HIPAA: 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 45 C.F.R. §164.308(a)(5)(ii); NIST SP: 800-50; OMB Memo: M-03-22, M-17-12;	**Related Controls Requirement(s):** AR-5, AR-6, AT-3, AT-4, PL-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security and privacy awareness and training policy, procedures addressing information security and privacy awareness training implementation, appropriate codes of federal regulations, information security and privacy awareness and training curricula, information security and privacy awareness and training materials, system security plan, personnel training records, training logs, and other relevant documents or records.
Examine: Organization implements automated information security and privacy awareness and training.
Interview: Organizational personnel with responsibilities for security awareness and training; organizational personnel with information security responsibilities; organizational personnel comprising the general information system user community.
Test: Automated mechanisms managing information security and privacy awareness and training.

AT-2(2)	Insider Threat (High, Moderate, Low)	Assurance	P1

Control:

The organization includes security awareness and training on recognizing and reporting potential indicators of insider threats, such as:
a. Inordinate, long-term job dissatisfaction,
b. Attempts to gain access to information not required for job performance,
c. Unexplained access to financial resources,
d. Bullying or sexual harassment of fellow employees,
e. Workplace violence, and
f. Other serious violations of organizational policies, procedures, directives, rules, or practices.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.

Supplemental Guidance:

Potential indicators and possible precursors of insider threat can include behaviors such 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 awareness and training includes how to communicate employee and management concerns regarding potential indicators of insider threats through appropriate organizational channels in accordance with established organizational policies and procedures.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** PL-4, PM-12, PS-3, PS-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security and privacy awareness and training policy; procedures addressing information security and privacy awareness and training implementation; appropriate codes of federal regulations; information security and privacy awareness and training curricula; information security and privacy awareness and training materials; system security plan; personnel training records; and other relevant documents or records.
Interview: Organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; and organizational personnel with information security responsibilities.

AT-3	Role-Based Security Training (High, Moderate, Low)	Assurance	P1

Control:

The organization provides role-based security training to personnel (both contractor and employee) with assigned information security and privacy roles and responsibilities (i.e., significant information security and privacy responsibilities):
a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. Within sixty (60) days of entering a position that requires role-specific training, and within every 365 days thereafter.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to CMS networks, systems, and/or applications; when required by significant information system or system environment changes; and when an employee enters a new position that requires additional role-specific training and refresher training within every three hundred sixty-five (365) days thereafter.
Std.2 - The minimal role-based security and privacy training received over a 365-day cycle must meet or exceed Federal/Departmental minimum requirements as described in the CMS Information System Security and Privacy Policy (IS2P2) role-based training (RBT) policy.
Std.3 - Information Security and Privacy awareness and training may be provided by CMS, or via a non-CMS FISMA system, or received by means of CMS- or HHS- approved RBT courses, professional development, certificate programs, and/or traditional college credit courses.
Std.4 - All CMS employees and contractors with significant information security roles and responsibilities that have not completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Provide role-based privacy training for all systems with PII, commensurate with the PII confidentiality impact level.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization provides information security and privacy refresher role-based training at least every three (3) years after initial RBT.

Supplemental Guidance:

Organizations determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals, the specific security 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 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, training on policies, procedures, tools, and artifacts for the organizational security and privacy 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 CMS's information security and privacy programs. Role-based security and privacy training also applies to contractors providing services to federal agencies.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Significant information security and privacy responsibilities are defined as the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the security and/or privacy posture of one or more CMS systems.

Reference(s): Code: 5 U.S.C. §552a(e)(9)-(10), Pub. L. No. 107-347, §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities;	**Related Controls Requirement(s):** AR-5, AR-6, AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16
HIPAA: 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.530(b)(2)(i); NIST SP: 800-16, 800-50; OMB Memo: M-03-22, M-17-12;	

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security and privacy awareness and training policy; procedures addressing information security and privacy training implementation; codes of federal regulations; security and privacy training curricula; information security and privacy training materials; system security plan; personnel training records; and other relevant documents or records.
Examine: Organization implements automated information security and privacy role-based training within required period.
Test: Automated mechanisms managing role-based information security and privacy training.

Systems defined as CSPs:

1. Records for FedRAMP approved systems are maintained by the sponsoring department/agency.
2. Evaluate adherence of systems deployed atop FedRAMP deployments to ARS basic requirements.

AT-4	Security Training Records (High, Moderate, Low)	Assurance	P3

Control:

The organization:
a. Identifies employees and contractors who hold roles with significant information security and privacy responsibilities;
b. Documents and monitors individual information system security and privacy training activities, including basic security and privacy awareness and training and specific role- based information system security and privacy training; and
c. Retains individual training records for a minimum of five (5) years after the individual completes each training.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization retains individual information security and privacy training records for at least three (3) years after the individual completes each training.

Supplemental Guidance:

Procedures and training implementation should:
a. Identify employees with significant information security and privacy responsibilities and provide role-specific training in accordance with NIST standards and guidance:
1. All users of CMS information systems must be exposed to security and privacy awareness materials at least every 365 days. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications;
2. Executives must receive training in information security and privacy basics and policy level training in security and privacy planning and management;
3. 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;
4. CIOs, 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; and
5. 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.
b. CMS must provide the CMS information systems security awareness material/exposure outlined in NIST guidance on information security awareness and training to all new employees before allowing them access to the systems;
c. CMS must provide information systems security and privacy refresher training for employees as frequently as CMS determines necessary, based on the sensitivity of the information that the employees use or process; and
d. CMS must 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.
e. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Maintaining security and privacy training records provides the capability for organizations to track compliance with privacy-related training requirements. Under HIPAA, a covered entity must document that the training as described within the regulation has been provided as required.

Reference(s): Code: 5 U.S.C. §552a(e)(9)-(10), Pub. L. No. 107-347, §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HIPAA: 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.530(b)(2)(ii) HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities OMB Memo: M-03-22, M-17-12;	**Related Controls Requirement(s):** AR-5, AR-6, AT-2, AT-3, PM-14

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security and privacy awareness and training policy; procedures addressing Information security and privacy training records; information security and privacy awareness and training records for personnel; and other relevant documents or records.
Examine: Organization implements automated required information security and privacy training records management.
Interview: Organizational personnel with information security and privacy training record retention responsibilities.
Test: Automated mechanisms supporting management of information security and privacy training records.

Systems defined as CSPs:

1. Records for FedRAMP approved systems are maintained by the sponsoring department/agency.
2. Evaluate adherence of systems deployed atop FedRAMP deployments to ARS basic requirements.

B.3 Audit and Accountability (AU)

AU-1	Audit and Accountability Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Reviews and updates (as necessary) the current:

1. Audit and accountability policy at least every three (3) years; and
2. Audit and accountability procedures at least every three (3) years.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Review and update (as necessary) the current audit and accountability policy in accordance with organizational policy but not less than every 365 days.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Security audit and accountability policies and procedures directly support privacy audit and accountability procedures.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D); NIST SP: 800-12, 800-100; OMB M-17-12, Circular A-130, 7.g., and 8.b(2)(c)	**Related Controls Requirement(s):** AU-2, AR-4, PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy and procedures; other relevant documents or records.
Interview: Organizational personnel with audit and accountability responsibilities.

AU-2	Audit Events (High, Moderate, Low)	P1

Control:

The organization:

a. Determines, based on a risk assessment and CMS mission/business needs, that the information system can audit the events specified in Implementation Standard 1;
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate (relevant) to support after-the-fact investigations of security and privacy incidents; and
d. Determines which events specified in Implementation Standard 2 require auditing on a continuous basis in response to specific situations.

Implementation Standards:

High & Moderate:

Std.1 - List of auditable events:
(a) Server alerts and error messages;
(b) User log-on and log-off (successful or unsuccessful);
(c) All system administration activities;
(d) Modification of privileges and access;
(e) Start up and shut down;
(f) Application modifications;
(g) Application alerts and error messages;
(h) Configuration changes;
(i) Account creation, modification, or deletion;
(j) File creation and deletion;
(k) Read access to sensitive information;
(l) Modification to sensitive information;
(m) Printing sensitive information;
(n) Anomalous (e.g., non-attributable) activity;
(o) Data as required for privacy monitoring privacy controls;
(p) Concurrent log on from different work stations;
(q) Override of access control mechanisms; and
(r) Process creation.
Std.2 - Subset of Implementation Standard 1 auditable events:
(a) User log-on and log-off (successful or unsuccessful);
(b) Configuration changes;
(c) Application alerts and error messages;
(d) All system administration activities;
(e) Modification of privileges and access;
(f) Account creation, modification, or deletion;
(g) Concurrent log on from different work stations; and
(h) Override of access control mechanisms.
Std.3 - Verify that proper logging is enabled to audit administrator activities.
Std.4 - Information collected will be compliant with the Federal Rules of Evidence.

Low:

Std.1 - List of auditable events:
(a) Server alerts and error messages;
(b) User log-on and log-off (successful or unsuccessful);
(c) All system administration activities;
(d) Modification of privileges and access;
(e) Start up and shut down;

(f) Application modifications;
(g) Application alerts and error messages;
(h) Configuration changes;
(i) Account creation, modification, or deletion;
(j) File creation and deletion;
(k) Read access to sensitive information;
(l) Modification to sensitive information;
(m) Anomalous (e.g., non-attributable) activity;
(n) Concurrent log on from different work stations;
(o) Override of access control mechanisms; and
(p) Process creation.

Std.2 - Subset of Implementation Standard 1 auditable events:
(a) User log-on and log-off (successful or unsuccessful);
(b) Configuration changes;
(c) Application alerts and error messages;
(d) All system administration activities;
(e) Modification of privileges and access;
(f) Account creation, modification, or deletion;
(g) Concurrent log on from different work stations; and
(h) Override of access control mechanisms.

Std.3 - Verify that proper logging is enabled to audit administrator activities.

Std.4 - Information collected will be compliant with the Federal Rules of Evidence.

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Determine that the information system can audit the following events:
(a) Monitor system access, including unsuccessful and successful login attempts, to information systems containing personally identifiable information (PII);
(b) Successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository;
(c) Privileged activities or system level access to PII;
(d) Concurrent logons from different workstations; and
(e) All program initiations, e.g., executable file.

PRIV.2 - Determine that the following events are to be audited within the information system:
(a) Monitor system access, including unsuccessful and successful login attempts, to information systems containing PII;
(b) Successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository;
(c) Privileged activities or system level access to PII;
(d) Concurrent logons from different workstations; and
(e) All program initiations, e.g., executable file.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - CSPs must implement this Standard (AU-2 CSP.1) as a replacement for the above Control (AU-2). The organization:
a. Determines, based on a risk assessment and mission/business needs, that the information system can audit the following events: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events; and for web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes; and
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;
c. Provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: organization-defined subset of the auditable events to be audited continually.
CSP.2 - For CSPs, the organization defines the subset of auditable events from AU-2a to be audited. The events to be audited are approved and accepted by the Joint Authorization Board (JAB).

Supplemental Guidance:

An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which 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, 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. Organizations consider in the definition of auditable events, 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.
The Federal Rules of Evidence can be found at this website: http://www.uscourts.gov/file/rules-evidence

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control identifies privacy-relevant security auditable events using a risk-based approach. Examples of privacy-relevant auditable events include logging access to or modification of PII.
The parameter values for this control do not provide an exhaustive list of all auditable events, but instead list the auditable events required by OMB privacy policy. The organization should manage the length of time that a log file is maintained to the period necessary to comply with the organization's security and privacy policies.

Guidance for systems processing, storing, or transmitting PHI:

The HIPAA Security Rule requires the auditing of activity in information systems that contain PHI but does not identify the specific audit events. Follow PII Supplemental Guidance.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R. §164.312(b), 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R; NIST SP: 800-37, 800-39, 800-92, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04, M-06-16, M-17-12; OMB Circular A-130, 7.g., 8.b(2)(c)(iii) and Appendix I; Web: csrc.nist.gov/pcig/cig.html	**Related Controls Requirement(s):** AC-6, AC-17, AR-4, AU-3, AU-12, MA-4, MP-2, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing auditable events; system security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records.
Examine: Information system implements defined auditing functionality. Examples:
- Auditing capability is installed, configured, and enabled;
- System is configured to capture information on network activity that cannot be attributed to a user or service;
- System and event logs are being collected as required and in the locations required; and
- Privileged applications are configured to capture system and event logs.
Interview: Organizational personnel with auditing and accountability responsibilities.
Test: Automated mechanisms implementing information system auditing of organization-defined auditable events. Examine audit trail data to ensure list of events defined under implementation standards are collected.

AU-2(3)	Reviews and Updates (High, Moderate)	P1

Control:

The organization reviews and updates the list of auditable events no less often than every three hundred sixty-five (365) days and whenever there is a significant system modification.

Implementation Standards:

High & Moderate:

Std.1 - The organization reviews and updates the list of auditable events as per the frequency defined in this control or whenever there is a change in the threat environment.

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (AU-2(3) CSP.1) as a replacement for the above Control Enhancement (AU-2(3)). The organization reviews and updates the list of auditable events at least every 365 days or whenever there is a change in the threat environment.

Supplemental Guidance:

Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing auditable events; system security plan; list of organization-defined auditable events; auditable events review and update records; information system audit records; information system incident reports; and other relevant documents or records.
Examine: Information system implements an update mechanism (automated or manual) for auditable events.
Interview: Organizational personnel with auditing and accountability responsibilities.
Test: Automated mechanisms supporting review and update of auditable events.

AU-3	Content of Audit Records (High, Moderate, Low)	P1

Control:

The information system generates audit records containing information that specifies:
- Date and time of the event;
- Component of the information system (e.g., software component, hardware component) where the event occurred;
- Type of event;
- User/subject identity;
- Outcome (success or failure) of the event;
- Execution of privileged functions; and
- Command line (for process creation events).

Implementation Standards:

Systems processing, storing, or transmitting PHI:

PHI.1 - Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify within every ninety (90) days for each extract that the data is erased or its use is still required.

Supplemental 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).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Audit records that are commensurate with the privacy risk they address are an effective tool for identifying whether, when, and how issues have occurred related to data quality and privacy breaches.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); OMB Memo: M-06-16, M-17-12 Att. 1 OMB Circular A-130: 7.g., and 8.b(2)(c)(iii)	**Related Controls Requirement(s):** AR-4, AU-2, AU-8, AU-12, SI-11

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PHI:

Determine if the organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; and other relevant documents or records.
Examine: Information system generates audit records containing required information. Examples:
- Auditing is enabled and active;
- Audit records contain the required information; and
- Applications, including network protocols, are configured to capture required information.

Test: Automated mechanisms implementing information system auditing of auditable events.

AU-3(1)	Additional Audit Information (High, Moderate)	P1

Control:

The information system generates audit records containing the following additional, more detailed information:
- Filename accessed;
- Program or command used to initiate the event; and
- Source and destination addresses.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (AU-3(1) CSP.1) as a replacement for the above Control Enhancement (AU-3(1)). The information system includes additional, more detailed session, connection, transaction, or activity duration information; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon in the audit records for audit events identified by type, location, or subject.
CSP.2 - For CSPs, the organization defines audit record types. The audit record types are approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system design documentation; system security plan; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system generates audit records containing required additional information.
Test: Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject.

AU-3(2)	Centralized Management of Planned Audit Record Content (High)	P1

Control:

The information system provides centralized management and configuration of the content to be captured in audit records generated by individual components throughout the information system.

Implementation Standards:

High:

Std.1 - Centralized audit repositories must be searchable by the CCIC:
(a) Information is available to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Centralized audit repository record sources include systems, appliances, devices, services, and applications (including databases).
Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.

Supplemental Guidance:

This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system.
Audit records contain evidence that can be used in the investigation of compromised systems. To prevent this evidence from being compromised, it must be sent to a separate system continuously. Methods for sending audit records include, but are not limited to, system audit tools used to send logs directly to another host or through the system's syslog service to another host.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AU-6, AU-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Examine: Information system provides centralized management and configuration of the content to be captured. Examples:
1. Audit data is collected and analyzed centrally within the organization; and
2. Audit data is available to the CCIC for analysis.

Test: Automated mechanisms implementing centralized management of audit record content.

AU-4	Audit Storage Capacity (High, Moderate, Low)	P1

Control:

The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Capacity must be sufficient to handle auditing records during peak performance times (e.g., open enrollment).

Supplemental 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 of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Adequate storage capacity for logs used to audit security- and privacy-related controls reduces the likelihood of the logs exceeding available storage space and potentially losing log information or reducing auditing capability. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act, and providing adequate storage capacity allows for preserving complete audit information for these purposes.

Reference(s): Code: 5 U.S.C. §552a(i); FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 164.312(b); OMB Memo: M-17-12; OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D)	**Related Controls Requirement(s):** AR-4, AU-2, AU-5, AU- 5(1), AU-6, AU-7, AU-9, AU-9(2), AU-11, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information system provides an appropriate storage capacity.
Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. Discuss auditing during peak system operation.
Test: Audit record storage capacity and related configuration settings.

AU-5	Response to Audit Processing Failures (High, Moderate, Low)	P1

Control:

The information system:
a. Alerts defined personnel or roles (defined in the applicable system security plan) in the event of an audit processing failure; and
b. Takes the actions defined in Implementation Standard 1 in response to an audit failure or audit storage capacity issue.

Implementation Standards:

High & Moderate:

Std.1 - Takes the following actions in response to an audit failure or audit storage capacity issue:
(a) Shutdown the information system or halt processing immediately; and
(b) Systems that do not support automatic shutdown must be shut down within 1 hour of the audit processing failure.

Low:

Std.1 - Takes the following actions in response to an audit failure or audit storage capacity issue:
(a) Shutdown the information system or halt processing;
(b) Stop generating audit records; or
(c) Overwrite the oldest records, in the case that storage media is unavailable.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For Moderate CSPs, the information system takes the following actions in the event of an audit processing failure: Shut down.
CSP.2 - For Low CSPs, the information system takes the following actions in the event of an audit processing failure: Overwrite oldest audit records.

Supplemental Guidance:

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2	**Related Controls Requirement(s):** AU-4, SI-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; system 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; and other relevant documents or records.
Examine: Information system provides an automated alerting on error/failure capability.
Test: Automated mechanisms implementing information system response to audit processing failures (i.e., halts processing or shuts down).

AU-5(1)	Audit Storage Capacity (High)	P1

Control:

The information system provides a warning to defined personnel, roles, and/or locations (defined in the applicable system security plan), within a defined time period (defined in the applicable system security plan), when allocated audit record storage volume reaches 80% of repository maximum audit record storage capacity.

Supplemental Guidance:

Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system provides an automated alerting on disk capacity threshold reached capability.
Test: Automated mechanisms implementing audit storage limit warnings.

AU-5(2)	Real-Time Alerts (High)	P1

Control:

The information system provides an alert in real-time to defined personnel, roles, and/or locations (defined in the applicable system security plan) when the following audit failure events occur:
- Record log is full;
- Auditing application reports an error;
- Authentication logging failure; and
- Encryption logging failure.

Supplemental Guidance:

Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system provides an automated alerting on error/failure capability.
Test: Automated mechanisms implementing real time audit alerts when organization-defined audit failure events occur.

AU-6	Audit Review, Analysis, and Reporting (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Reviews and analyzes information system audit records no less often than weekly for indications of inappropriate or unusual activity as defined within the Implementation Standards; and
b. Reports findings to defined personnel or roles (defined in the applicable system security plan).

Implementation Standards:

High:

Std.1 - Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment.
Std.2 - Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty- four (24) hour period and on demand. Generate alerts for technical personnel review and assessment.
Std.3 - Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
Std.4 - Use automated utilities to review audit records no less often than once every twenty-four (24) hours for unusual, unexpected, or suspicious behavior.
Std.5 - Inspect administrator groups on demand but no less often than once every seven (7) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.
Std.6 - Perform manual reviews of system audit records randomly on demand but no less often than once every thirty (30) days.

Moderate:

Std.1 - Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment.
Std.2 - Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty- four (24) hour period and on demand. Generate alerts for technical personnel review and assessment.
Std.3 - Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
Std.4 - Use automated utilities to review audit records no less often than once every seventy-two (72) hours for unusual, unexpected, or suspicious behavior. **Std.5 -** Inspect administrator groups on demand but no less often than once every fourteen (14) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.
Std.6 - Perform manual reviews of system audit records randomly on demand but no less often than once every thirty (30) days.

Low:

Std.1 - Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment.
Std.2 - Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty- four (24) hour period and on demand. Generate alerts for technical personnel review and assessment.
Std.3 - Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
Std.4 - Use automated utilities to review audit records no less often than every seventy-two (72) hours for unusual, unexpected, or suspicious behavior.
Std.5 - Inspect administrator groups on demand but no less often than once every thirty (30) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.
Std.6 - Inspect administrator groups on demand but no less often than once every thirty (30) days to ensure unauthorized administrator accounts have not been created.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - Use automated utilities to review audit records no less often than defined under the DHS Continuous Diagnostics and Mitigation and NIST continuous monitoring direction for unusual, unexpected, or suspicious behavior.
CSP.2 - For CSPs, the organization reviews and analyzes information system audit records no less often than defined under the DHS Continuous Diagnostics and Mitigation and NIST continuous monitoring direction for indications of inappropriate or unusual activity, and reports findings to designated organizational officials. **CSP.3 -** For CSPs, 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.

Supplemental 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Periodic reviews and analysis of privacy logs are important for identifying indications of inappropriate or unusual activity that may signify a privacy incident or breach.

Reference(s): Code: 5 U.S.C. §552a(g)(1)(D); FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R. §164.312(b); NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-7-16, M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AC-2, AC-3, AC-6, AC-17, AR-4, 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

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

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; and other relevant documents or records.
Examine: Information system provides an anomalous behavior detection and reporting capability.
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.
Test: Use automated utilities in the review of audit records.
Test: Information system audit review, analysis, and reporting capability.

AU-6(1)	Process Integration (High, Moderate)	Assurance	P1

Control:

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Implementation Standards:

High & Moderate:

Std.1 - Aggregated audit records from automated information security capabilities and service tools must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Audit records sources include systems, appliances, devices, services, and applications (including databases).
(c) CCIC directed audit information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.
Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Supplemental Guidance:

Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AU-12, PM-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information system provides automated mechanisms to integrate audit review, analysis, and reporting processes to support investigation and response to suspicious activities.
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.
Test: Information system capability integrating audit review, analysis, and reporting into an organizational process for investigation and response to suspicious activities.

AU-6(3)	Correlate Audit Repositories (High, Moderate)	Assurance	P1

Control:

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Implementation Standards:

High & Moderate:

Std.1 - Correlated results from automated tools must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Repository sources include systems, appliances, devices, services, and applications (including databases); and
(c) CCIC directed repository information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.
Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Supplemental 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.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Correlating and analyzing privacy audit logs across different log repositories and systems provides greater awareness of privacy incidents and breaches across the organization.

Reference(s): Code: 5 U.S.C. §552a(g)(1)(D); FedRAMP Rev. 4 Baseline; OMB Memo: M-7-16	**Related Controls Requirement(s):** AU-12, IR-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information system provides the capability to analyze and correlate audit records generated across different repositories.
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.
Test: Automated mechanisms integrating audit review, analysis, and reporting processes.

AU-6(5)	Integration/Scanning and Monitoring Capabilities (High)	Assurance	P1

Control:

The organization integrates analysis of audit records with analysis of (one-or-more, defined in the applicable system security plan): vulnerability scanning information; performance data; information system monitoring information; and/or other defined data/information (defined in the applicable system security plan) collected from other sources, to further enhance the ability to identify inappropriate or unusual activity.

Implementation Standards:

High:

Std.1 - Aggregated vulnerability scanning information, performance data, and network monitoring information from automated tools must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include systems, appliances, devices, services, and applications (including databases); and
(c) CCIC directed information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. **Std.2 -** As required by CMS, raw vulnerability scanning information, performance data, and network monitoring information must be available in an unaltered format to the CCIC.
Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Supplemental Guidance:

This control enhancement does not require vulnerability scanning, the generation of performance data, or information system monitoring. Rather, the control enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can help uncover denial of service attacks or cyber-attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations. Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AU-12, IR-4, RA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; integrated analysis of audit records, vulnerability scanning information, performance data, network monitoring information and associated documentation; and other relevant documents or records.
Examine: Information system provides the capability to analyze and correlate audit records with analysis of vulnerability scanning information, performance data, and network monitoring information.
Test: Information system capability for centralizing review and analysis of audit records from multiple information system components. Audit records with analysis of vulnerability scanning information, performance data, and network monitoring information must be analyzed for relevant security and privacy alerts. Additionally, collected information must be made available to the CCIC for aggregation and analysis at the CMS enterprise level.

AU-6(6)	Correlation with Physical Monitoring (High)	Assurance	P1

Control:

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Supplemental Guidance:

The correlation of physical audit information and audit logs from information systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain information systems with the additional physical security information that the individual was present at the facility when the logical access occurred, may prove to be useful in investigations.
- Cross-organizational coordination leverages critical information from a variety of sources to more effectively respond to information security-related incidents that potentially affect organization operations, assets, and individuals.
- The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns.
- Effectiveness of event correlation depends on the quality of the data that goes into it. Organizations should establish logging standards and procedures to ensure that adequate information is collected and that the data is reviewed regularly.
- Consistent log timestamps facilitate effective event correlation.

Reference(s): NIST SP: 800-100, 800-61	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; system security plan; and other relevant documents or records.
Examine: Information system provides the capability to analyze and correlate required security data.
Test: Information system capability for centralizing review and analysis of audit records from multiple information system components.

AU-7	Audit Reduction and Report Generation (High, Moderate)	Assurance	P2

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.

Supplemental 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.
- Event collection and analysis software can perform event reduction by disregarding data that are not significant to information system security, potentially increasing its efficiency in network and storage resource needs.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

To meet the deadlines associated with reporting loss of sensitive information, such as a breach of personally identifiable information (PII), it is necessary to can summarize audit information and generate customized audit reports.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.312(b) NIST SP: 800-137; OMB Memo: M-17-12, Att. 2	**Related Controls Requirement(s):** AU-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; and other relevant documents or records.
Examine: Information system provides an audit reduction and report generation capability that meets defined requirements.
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.
Test: Audit reduction and report generation capability.

AU-7(1)	Automatic Processing (High, Moderate)	Assurance	P2

Control:

The information system provides the capability to process audit records for events of interest based on selectable event criteria.

Supplemental 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

To conduct efficient and effective remediation of loss of sensitive information, such as a breach of personally identifiable information (PII), it may be necessary to tailor the audit fields provided in audit reports. For example, it may be necessary to include the identities of individuals and the system resources involved to determine scope of access to an information system containing the sensitive information. However, consideration must be given on admissibility as defined by the Federal Rules of Evidence.
The Federal Rules of Evidence can be found at this website: http://www.uscourts.gov/file/rules-evidence

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-17-12, Att. 2; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)	**Related Controls Requirement(s):** AU-2, AU-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; information system audit records; and other relevant documents or records.
Examine: Information system provides the capability to analyze and correlate required security data on defined criteria.
Test: Audit reduction and report generation capability.

AU-7(2)	Non-Mandatory: Automatic Sort and Search	P3

Control:

The information system provides the capability to sort and search audit records for events of interest based on the content of organization-defined audit fields within audit records.

Supplemental Guidance:

Sorting and searching of audit records may be based upon the contents of audit record fields, for example: (i) date/time of events; (ii) user identifiers; (iii) Internet Protocol (IP) addresses involved in the event; (iv) type of event; or (v) event success/failure.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

To conduct efficient and effective remediation of loss of sensitive information, such as a breach of personally identifiable information (PII), it may be necessary to tailor the organization of the audit report or to provide search functionality with audit reports that are generated. For example, if the PII breach involves only one or two users it may be most efficient to sort the audit report by user ID or to provide the ability to search on user ID within the audit report. Consideration must be given on admissibility as defined by the Federal Rules of Evidence.

The Federal Rules of Evidence can be found at this website: http://www.uscourts.gov/file/rules-evidence

Reference(s): OMB Memo: M-17-12, Att. 2; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:

(i) the organization defines audit fields within audit records to sort and search audit records for events of interest based on content of such audit fields; and
(ii) the information system provides the capability to sort and search audit records for events of interest based on the content of organization-defined audit fields within audit records.

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; audit record criteria (fields) establishing events of interest; information system audit records; other relevant documents or records.
Examine: Information system provides the capability to analyze and correlate required security data on defined criteria.
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.

AU-8	Time Stamps (High, Moderate, Low)	P1

Control:

The information system:

a. Uses internal system clocks to generate time stamps for audit records; and
b. Records time stamps for audit records that can be mapped to UTC or Greenwich Mean Time (GMT) and is accurate to within one hundred (100) milliseconds.

Supplemental 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.

- The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns; and
- Consistent log timestamps facilitate effective event correlation.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2	**Related Controls Requirement(s):** AU-3, AU-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; or other relevant documents or records.
Examine: Information system provides required time stamping and synchronization.
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.
Test: Audit reduction and report generation capability.

AU-8(1)	Synchronization with Authoritative Time Source (High, Moderate)	P1

Control:

The information system:
a. Compares the internal information system clocks no less often than daily and at system boot with one or more of the following federally maintained NTP stratum-1 servers:
- NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi)
- U.S. Naval Observatory Stratum-1 NTP Servers (http://tycho.usno.navy.mil/ntp.html); and
- CMS designated internal NTP time servers providing an NTP Stratum-2 service to the above servers; and
b. Synchronizes the internal clocks to the authoritative time source when the time difference is greater than one hundred (100) milliseconds.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the information system synchronizes internal information system clocks at least hourly with: http://tf.nist.gov/tf-cgi/servers.cgi.
CSP.2 - For CSPs, the organization selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.
CSP.3 - For CSPs, 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.

Supplemental Guidance:

This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.
- The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns; and
- Consistent log timestamps facilitate effective event correlation.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-61, 800-100	**Related Controls Requirement(s):** AU-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing time stamp generation; system security plan; information system design documentation; information system configuration settings and associated documentation; or other relevant documents or records.
Examine: Information system provides required time stamping and synchronization.
Test: Automated mechanisms implementing internal information system clock synchronization.

AU-9	Protection of Audit Information (High, Moderate, Low)	P1

Control:

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Implementation Standards:

High:

Std.1 - Cryptographic mechanisms shall be employed to protect the integrity of audit information (e.g. log, and audit tools).

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When audit information contains sensitive information, such as personally identifiable information (PII) or protected health information (PHI), it must be protected commensurate with the information's confidentiality impact level. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act. Protecting audit records from compromise by applying this control enhancement helps ensure their availability when needed.

Reference(s): Code: 5 U.S.C. §552a(i); FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; OMB Memo: M-17-12; OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)	**Related Controls Requirement(s):** AC-3, AC-6, AU-4(1), MP-2, MP-4, PE-2, PE-3, PE-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; and other relevant documents or records. **Examine:** Information system is configured to protect audit tools and data from unauthorized access.
Test: Automated mechanisms implementing audit information protection. Examine tools, data files. Ensure file rotations retain required protections.

AU-9(2)	Audit Backup on Separate Physical Systems/Components (High)	P1

Control:

The information system backs up audit records no less often than weekly onto a physically different system or system component than the system or component being audited.

Implementation Standards:

High:

Std.1 - The centralized audit servers must meet this control.
Std.2 - The centralized audit server must be separated from the audit client information systems.

Supplemental Guidance:

This control is satisfied for servers forwarding audit records and information to a centralized audit server for aggregation and analysis.

Guidance for systems defined as CSPs:

This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-137	**Related Controls Requirement(s):** AU-4, AU-5, AU-11

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing protection of audit information; system security plan; information system design documentation; information system configuration settings and associated documentation, system or media storing backups of information system audit records; information system audit records; and other relevant documents or records.
Examine: The information system backs up audit records onto a physically different system or system component than the system or component being audited.
Interview: Organizational personnel with auditing and accountability responsibilities.

AU-9(3)	Cryptographic Protection (High)	P1

Control:

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Supplemental Guidance:

Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Using cryptographic mechanisms protects audit log integrity and the confidentiality of the information in the logs, including information related to privacy incidents and breaches. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act.
In addition to cryptographic mechanisms to protect integrity, the confidentiality of personally identifiable information (PII) may require the use of encryption.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

Reference(s): Code: 5 U.S.C. §552a(i); OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.306(a)(1); 45 C.F.R. §164.312(a)(2)(iv)	**Related Controls Requirement(s):** AU-10, SC-12, SC-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; and other relevant documents or records.
Examine: Information system implements FIPS 140-2-validated cryptographic mechanisms to protect the integrity of audit information.
Interview: Organizational personnel with auditing and accountability responsibilities.

AU-9(4)	Access by Subset of Privileged Users (High, Moderate)	P1

Control:

The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system, and is defined in the applicable system security plan.

Supplemental Guidance:

Individuals with privileged access to an information system and 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When audit information contains personally identifiable information (PII), the requirement for access to that audit information is the same as for access to PII generally. As such, access to PII in audit logs requires a need-to-know and privacy training commensurate with level of responsibility and access. Privileged users must be evaluated to determine if they have such a need-to-know as part of his or her security function.

Reference(s): Code: 5 U.S.C. §552a(b)(1); FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AC-5, AR-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; and other relevant documents or records. **Interview:** Organizational personnel with auditing and accountability responsibilities.

AU-10	Non-Repudiation (High)	Assurance	P2

Control:

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed a particular action.

Supplemental Guidance:

Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an 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).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Non-repudiation is a critical element of accountability and accuracy of information in system history and logs, and it is important for investigating incidents and breaches.

Reference(s): Code: 5 U.S.C. §552a(e)(5) and (g)(1)(c); FISCAM: AC-2, AS-2; OMB Circular A-130: 7.g. and 8.b(2)(c)(iii); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(c)(2); 45 C.F.R. §164.312(e)(2)(i)	**Related Controls Requirement(s):** AR-4, AR-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information system limits access to audit capabilities to authorized users and protects data from unauthorized modification.
Test: Automated mechanisms implementing non-repudiation capability.

AU-11	Audit Record Retention (High, Moderate, Low)	P3

Control:

The organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and CMS information retention requirements.

Implementation Standards:

High, Moderate, & Low:

Std.1 - When subject to a legal investigation (e.g., Insider Threat), audit records must be maintained until released by the investigating authority.
Std.2 - Audit record retention must comply with National Archives and Records Administration (NARA) or other authoritative mandate durations.

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Audit inspection reports, including a record of corrective actions, must be retained by the organization for a minimum of three (3) years from the date the inspection was completed.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization retains audit records on-line for at least ninety (90) days and further preserves audit records off-line for a period that is in accordance with NARA requirements.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HHS: Policy for Monitoring Employee Use of HHS IT Resources	**Related Controls Requirement(s):** AU-4, AU-5, AU-9, MP-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing audit record retention; system security plan; organization-defined retention period for audit records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with information system audit record retention responsibilities.

AU-12	Audit Generation (High, Moderate, Low)	P1

Control:

The information system:

a. Provides audit record generation capability for the following auditable events defined in AU-2a:
- All successful and unsuccessful authorization attempts;
- All changes to logical access control authorities (e.g., rights, permissions);
- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
- The audit trail, which must capture the enabling or disabling of audit report generation services; and
- The audit trail must capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

b. Allows defined personnel or roles (defined in the applicable system 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:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, 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.

Supplemental 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 can generate audit records.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control defines the technical aspects of how the privacy auditing requirements identified in controls AU-2 and AU-3 will be selected, generated and reviewed for compliance.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g. and 8.b(2)(c)(iii); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b)	**Related Controls Requirement(s):** AC-3, AU-2, AU-3, AU-6, AU-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Audit and accountability policy; procedures addressing audit record generation; system security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system provides the required audit record generation capability.
Interview: Organizational personnel with information system audit record generation responsibilities.
Test: Automated mechanisms implementing audit record generation capability.

AU-12(1)	System-Wide/Time-Correlated Audit Trail (High)	P1

Control:

The information system compiles audit records from defined information system components (defined in the applicable system security plan) into a system-wide (logical or physical) audit trail that is time-correlated to within +/- five (5) minutes.

Supplemental 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.

Reference(s):	Related Controls Requirement(s): AU-8, AU-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; information system audit records; and other relevant documents or records.
Examine: Information system aggregates, correlates, and compiles audit records from client systems in a manner that supports defined time variance.
Test: Automated mechanisms implementing audit record generation capability.

AU-12(3)	Changes by Authorized Individuals (High)	P1

Control:

The information system provides the capability for defined individuals or roles (defined in the applicable system security plan) to change the auditing to be performed on defined information system components (defined in the applicable system security plan) based on defined selectable event criteria (defined in the applicable system security plan) within minutes.

Systems processing, storing, or transmitting PII (to include PHI):

The information system provides the capability for a limited subset of authorized system administrators to change the auditing to be performed on any information system that contains PII based on change in risk based on law enforcement, intelligence, or other credible sources of information or a security incident within minutes.

Supplemental Guidance:

This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Changes to the audit of information systems containing sensitive information must be limited to a subset of authorized system administrators to ensure integrity of audit logs. This control requires organization to define the individuals or roles that would be able to make changes to audit generation requirements.

Reference(s): OMB Circular A-130: 7.g. and 8.b(2)(c)(iii); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R.§164.308(a)(2)	Related Controls Requirement(s): AU-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; information system audit records; and other relevant documents or records.
Examine: Information system provides the capability for defined individuals or roles to change the auditing to be performed.
Interview: Organizational personnel with information system audit record generation responsibilities.

B.4 Security Assessment and Authorization (CA)

CA-1	Security Assessment and Authorization Policies and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and.

b. Reviews and updates (as necessary) the current:

1. Security assessment and authorization policy at least every three (3) years; and
2. Security assessment and authorization procedures at least every three (3) years.

Supplemental 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 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The security assessment and authorization policy and procedures should address the strategy for including applicable privacy requirements and controls in the security program and information systems.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(8); HSPD 7: F(19); NIST SP: 800-12, 800-37, 800-100; OMB Memo: M-17-12, Att. 1; 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(1)(ii); 45 C.F.R. §164.316(b)(2)(ii); 45 C.F.R. §164.308(a)(2)	**Related Controls Requirement(s):** AR-1, AR-7, PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policies and procedures; other relevant documents or records.
Interview: Organizational personnel with security assessment and authorization responsibilities.

CA-2	Security Assessments (High, Moderate, Low)	Assurance	P2

Control:

The organization:

a. Develops an information security and privacy control assessment plan that describes the scope of the assessment including:

1. Security and privacy controls and control enhancements under assessment (including information security and privacy changes enacted by HHS and CMS CIO/CISO directives);
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, as defined in implementation standards, within every three hundred sixty-five (365) days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard 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 and privacy requirements;

c. Produces an assessment report that documents the results of the assessment; and

d. Provides the results of the security and privacy control assessment within thirty (30) days after its completion, in writing, to the Business Owner responsible for the system and personnel responsible for reviewing the assessment documentation, and updating system security documentation where necessary to reflect any changes to the system.

Implementation Standards:

High, Moderate, & Low:

Std.1 - An assessment of all controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems.
Std.2 - The annual assessment requirement mandated by OMB requires all baseline controls CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs must be tested each year so that all security controls are tested during a 3-year period.
Std.3 - The Business Owner notifies the CMS CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, Information System Security Officer [ISSO]).

Supplemental Guidance:

Organizations assess security controls in organizational information system and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from NIST SP 800-53 Appendix F (main catalog) and NIST SP 800-53 Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by CMS, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The Federal Information Security Modernization Act (FISMA) requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.
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 assessment results are current, relevant to the determination of security control effectiveness; and obtained with the appropriate level of assessor independence. Existing security 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.
After initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security 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 CMS operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the FISMA annual assessment requirement if the results are current, valid, and relevant to determining security 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control addresses the process of planning for and executing security assessments, the scope of which should include assessment of applicable privacy requirements.

Once the final security assessment is completed, update the associated Privacy Impact Assessment (PIA) to reflect the results of the security assessment.

Reference(s): Code: 5 United States Code (U.S.C.) §552a(b); Executive Order: 13587; FedRAMP Rev. 4 Baseline; Federal Information Processing Standard (FIPS) Pub: 199; FISCAM: AS-1, SM-5; HIPAA: 45 C.F.R. §164.308(a)(8); HSPD 7: D(11), F(19); NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-17-12 Att. 1, A.2.c, M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AR-2, CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment policy; procedures addressing security assessments; system security plan; security assessment plan; assessment evidence; and other relevant documents or records.
Examine: Information system is assessed in accordance with the assessment plan.

CA-2(1)	Independent Assessors (High, Moderate)	Assurance	P2

Control:

The organization employs assessors or assessment teams with CMS CISO defined level of independence to conduct security control assessments.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization employs an independent assessor or assessment team to assess the security controls in the information system.

Supplemental Guidance:

Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding 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 being 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.
AOs determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. AOs also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk- based decisions. This includes determining whether 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 be conducted by individuals that 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 useable for such decisions, thereby reducing the need to repeat assessments.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; procedures addressing security assessments; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); and other relevant documents or records.
Interview: Organizational personnel with security assessment responsibilities.

CA-2(2)	Specialized Assessments (High)	P2

Control:

The organization includes as part of security control assessments, within every three hundred sixty-five (365) days, announced or unannounced in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; and performance/load testing.

Implementation Standards:

High & Moderate:

Std.1 - Announced or unannounced in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) In-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing result information sources include traffic analysis tool systems, appliances, devices, services, and applications; and
(c) CCIC directed in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw results from in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing must be available in an unaltered format to the CCIC.
Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Supplemental Guidance:

Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** PE-3, SI-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; procedures addressing security assessments; system security plan; security assessment plan; security assessment report; assessment evidence; and other relevant documents or records.
Interview: Organizational personnel with security assessment responsibilities.

CA-2(3)	External Organizations (High)	P2

Control:

The organization accepts the results of an assessment of CMS information systems performed by CMS authorized independent assessors when the assessment meets CMS defined requirements and methodologies for performing assessments.

Supplemental Guidance:

Organizations may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for organizational assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations may consider in determining whether to accept assessment results from external organizations can vary.
Determinations for accepting assessment results can be based on, for example, past assessment experiences one organization has had with another organization, the reputation that organizations have about assessments, the level of detail of supporting assessment documentation provided, or mandates imposed upon organizations by federal legislation, policies, or directives.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M- 16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; procedures addressing security assessments; system security plan; security assessment plan; security assessment report; assessment evidence; and other relevant documents or records.
Examine: Information detailing how assessment results are recorded and tracked. Example:
- Is the organization actively using CFACTS to track results?
- Is the organization remediating open findings being tracked?
Interview: Organizational personnel with security assessment responsibilities.

CA-3	System Interconnections (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Authorizes connections from the information system to other information systems using Interconnection Security Agreements (ISA) or other comparable agreements (such as MOU/MOA, SLA, or specific contractual clause, so long as the appropriate interconnection detail is provided therein);
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated;
c. Reviews and updates the interconnection agreements no less often that once every year and whenever significant changes (that can affect the security state of the information system) are implemented that could impact the validity of the agreement as a verification of enforcement of security requirements; and
d. Only activates a system interconnection (including testing) when a signed interconnection agreement is in place.

Implementation Standards:

High, Moderate, & Low:

Std.1 - If the interconnecting systems have the same AO (or same primary operational IT infrastructure manager), an interconnection agreement document is not required; rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems.
Std.2 - Record each system interconnection in the applicable security plan and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.
Std.3 - The interconnection agreement (or other applicable connection agreement) is updated following significant changes to the system, organizations, or the nature of the electronic sharing of information that could impact the validity of the agreement.
Std.4 - The CMS CIO, CISO, and Senior Official for Privacy (SOP) have the authority to order the immediate termination and/or suspension of any interconnection that, in the judgment of the CMS officer and CMS Security Operations, presents an unacceptable level of risk to the CMS enterprise and/or mission.
Std.5 - The interconnection agreement must be fully signed and executed prior to any interconnection outside of the system boundary taking place for any purpose (within the constraints of the control [e.g., dedicated connections], including testing).

Supplemental 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 CMS authorizing official determines the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same CMS Authorizing Official, an Interconnection Security Agreement (ISA) or another specific interconnection document (such as MOU/MOA, SLA, or specific contractual clause) is not required. Interface characteristics between the interconnecting information systems can be described in the security plans for their respective systems. Instead of developing an interconnection agreement (or other valid interconnection agreement forms such as MOU/MOA, SLA, etc.), organizations may choose to incorporate this information into formal contracts (so long as the appropriate detail is provided therein), especially if the interconnection is to be established between CMS and a non-federal (private sector) organization. Risk considerations also include information systems sharing 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 interconnection agreements and be subject to additional security controls.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Interconnection agreements document whether and under what circumstances sensitive information, such as personally identifiable information (PII), can be shared between information systems in different authorization boundaries (e.g., an interface between systems owned by different agencies) over a dedicated or "always on" connection. Interconnection agreements communicate that sensitive information will be communicated via the connection and define the security parameters required to protect it. Interconnection agreements also provide a record of agreed upon terms and a document against which controls can be enforced and audited. Organizational policy dictates whether interconnection agreements are required for internal connections within an organization.

Guidance for systems processing, storing, or transmitting PHI:

Consider the need for a MOU/MOA or Business Associate Agreement, and implement as necessary.

Reference(s): Code: 5 U.S.C. §552a(o); FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-1, AS-2; HIPAA: 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.308(b)(4), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.308(b)(3); 45 C.F.R. §164.504(e)(3); HSPD 7:F(19); NIST SP: 800-47	**Related Controls Requirement(s):** AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; system security plan; information system design documentation; security assessment report; plan of action and milestones; MOUs and SLAs (as appropriate); and other relevant documents or records.
Examine: Details about system interconnections.
Interview: Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements.

CA-3(5)	Restrictions on External System Connections (High, Moderate)	P1

Control:

The organization employs, and documents in the applicable system security plan, a deny-all, permit-by-exception, policy for allowing defined information systems (defined in the applicable security plan) to connect to external information systems.

Supplemental Guidance:

Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies regarding such connectivity: (i) allow-all, deny by exception, also known as blacklisting (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as whitelisting (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable.

Systems processing, storing, or transmitting PII (to include PHI):

External network connections open the opportunity for intentional as well as inadvertent disclosure of sensitive information, such as personally identifiable information (PII). Email and file sharing applications are common points of vulnerability. Organizations require the ability to evaluate external network connections on a case-by-case basis to ensure such connections do not permit unauthorized access or disclosure of sensitive information.

Reference(s): Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; OMB Memo: M-17-12; 45 C.F.R. §164.312(a)(1)	**Related Controls Requirement(s):** CM-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; system security plan; information system design documentation; security assessment report; plan of action and milestones; and other relevant documents or records.
Interview: Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements.

CA-5	Plan of Action and Milestones (High, Moderate, Low)	Assurance	P3

Control:

The organization:
a. Develops and submits a POA&M for the information system within thirty (30) days of the submission of final results (e.g., Final Report) for every internal/external audit/review or test (e.g., Security Control Assessment [SCA], penetration test, automated configuration and vulnerability scan results) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates and submits existing POA&Ms monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance:

POA&Ms are key documents in security authorization packages and are subject to federal reporting requirements established by OMB.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-6; HIPAA: 45 C.F.R. §164.308(a)(2), 45 C.F.R. §164.308(a)(8); HSPD 7: F(19), G(24); NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-02-01, M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** 2, CA-7, CM-4, PM-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; procedures addressing plan of action and milestones; system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; and other relevant documents or records.
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.

CA-6	Security Authorization (High, Moderate, Low)	Assurance	P3

Control:

The organization: Authorizing Official (AO) authorizes the information system for processing prior to commencing any operations; and

a. Updates the security authorization:
- Within every three (3) years;
- When significant changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements that impact the system;
- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
- Prior to expiration of a previous security authorization.

Implementation Standards:

High, Moderate, & Low:

Std.1 - The organization must notify the CCIC of significant changes to architecture, security posture, or other items that could cause degradation or unexpected results in security monitoring, detection, response, and mitigation activities prior to making a change.

Supplemental Guidance:

Security authorizations are official management decisions, conveyed through authorization decision documents, by the CMS CIO or his/her designated representative (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to CMS 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 CMS CIO or his/her designated representative prior to a system being placed into operations. Through the security authorization process, the CMS CIO is accountable for security risks associated with the operation and use of CMS information systems.

OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing the CMS CIO and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, the CMS CIO uses results of the continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

One of the considerations for the “go/no go” decision when authorizing (or re-authorizing) an information system is whether applicable privacy requirements have been met.

Guidance for systems processing, storing, or transmitting PHI:

The senior-level executive should be one of the following: HIPAA Security Officer, Authorizing Official, Program Manager, Information System Security Manager (ISSM), or Information System Security Officer (ISSO).

Guidance for systems defined as CSPs:

Significant change is defined in NIST SP 800-37 Revision 1, Appendix F. The CSP describes the types of changes to the information system or the environment of operations that would require a reauthorization of the information system. The types of changes are approved and accepted by the Joint Authorization Board (JAB).

Reference(s): Code: Pub. L. No. 107-347, §208; 5 U.S.C. §552a(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS- 1, SM-2; HIPAA: 45 C.F.R. §164.308(a)(2); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(2)(iii); HSPD 7: F(19); NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-11-33, M-14-03, M-15-01, M-16-04; OMB Circular A-130	**Related Controls Requirement(s):** CA-1, CA-2, CA-7, PM-9, PM-10

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; authorization statement); and other relevant documents or records.
Interview: Organizational personnel with security authorization responsibilities

CA-7	Continuous Monitoring (High, Moderate, Low)	Assurance	P3

Control:

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. Establishment of defined metrics (defined in the applicable system security plan) to be monitored based on the organization security goals and objectives and in accordance with the basic requirements set forth in NIST SP 800-137;
b. Establishment of defined frequencies (defined in the applicable system security plan), but no less than once every 72 hours, for monitoring and defined frequencies (defined in the applicable system security plan), but no less than once every 72 hours, for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-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; and
g. Reporting the security status of the organization and the information system to defined personnel or roles (defined in the applicable system security plan) monthly.

Implementation Standards:

High, Moderate, & Low:

Std.1 - When subject to a legal investigation (e.g., of an insider threat), continuous monitoring records must be maintained until released by the investigating authority.
Std.2 - Monitors systems, appliances, devices, and applications (including databases).
Std.3 - The CCIC provides oversight of information security and privacy, to include Security Information and Event Management (SIEM), for each FISMA System operating by or on behalf of CMS.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The state of security controls can directly correlate to privacy risk. Continuous monitoring supports the identification of issues that could result in unauthorized access to sensitive information such as PII, data quality issues, and other concerns, including privacy, that are supported by security controls.

Guidance for systems processing, storing, or transmitting PHI:

Consider using automated tools and mechanisms for system activity review. The effectiveness of continuous monitoring of various activities, for example, failed or successful log-ins, inappropriate file access, detecting and reporting on malicious code/viruses through network transmission, is enhanced using approved automated tools.

Reference(s): Code: 5 U.S.C. §552a(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-5; HHS: Policy for Monitoring Employee Use of HHS IT Resources; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.308(a)(5)(ii)(C) HSPD 7: F(19); NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-11-33, M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AR-4, CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; system security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; and other relevant documents or records.
Examine: Information system is integrated into organizational and CMS continuous monitoring program.
Interview: Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities.

CA-7(1)	Independent Assessment (High, Moderate)	Assurance	P2

Control:

The organization employs assessors or assessment teams with CMS CISO defined level of independence to monitor the security controls in the information system on an ongoing basis.

Supplemental Guidance:

Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. 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 being 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. An independent assessor (defined in the RMH, *Volume 1, Chapter 10, CMS Risk Management Terms, Definitions, and Acronyms*) may be any internal/external agent or team that can conduct an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain-of-command associated with the information system or to the determination of control effectiveness. Since these determinations are somewhat subjective, the CMS CISO retains the ultimate authority to make final judgments on the independence of any assessor. In addition, see CMS IS2P2 section entitled Risk Management Framework RMF (CMS-RMF-1.8).

Reference(s): FedRAMP Rev. 4 Baseline; HSPD 7: F(19); NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AC-9, CA-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with continuous monitoring responsibilities

CA-8	Penetration Testing (High and Moderate HVA systems)	P2

Control:

The organization conducts both internal and external penetration testing, within every three hundred sixty-five (365) days, on defined information systems or system components (defined in the applicable system security plan), or whenever there has been a significant change to the system. As a minimum, penetration testing must be conducted to determine:
a. How well the system tolerates real world-style attack patterns;
b. The likely level of sophistication an attacker needs to successfully compromise the system;
c. Additional countermeasures that could mitigate threats against the system; and
d. Defenders' ability to detect attacks and respond appropriately.
Penetration testing is required under OMB M-17-09 for all systems defined as High Value Assets (HVAs)

Implementation Standards:

High:

Std.1 - Conduct internal and external penetration testing as needed but no less often than once every three hundred sixty-five (365) days in accordance with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements.
Std.2 - Penetration tests are performed when new risks and threats potentially affecting the system/applications are identified and reported or upon request from CMS. **Std.3 -** Penetration test scanning includes evaluation of embedded structures (e.g., content that can be changed without reloading the anchor content) and interactive content.
Std.4 - Penetration test scanning results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Penetration test information sources include systems, appliances, devices, services, and applications (including databases).
(c) CCIC directed penetration test information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.5 - Penetration testing on a production system must be conducted in a manner that minimized risk of information corruption or service outage.
Std.6 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Moderate & Low:

Std.1 – When selected, conduct internal and external penetration testing as needed but no less often than once every three hundred sixty-five (365) days in accordance with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements.
Std.2 – When selected, penetration tests are performed when new risks and threats potentially affecting the system/applications are identified and reported or upon request from CMS.
Std.3 – When selected, penetration test scanning includes evaluation of embedded structures (e.g., content that can be changed without reloading the anchor content) and interactive content.
Std.4 – When selected, penetration test scanning results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Penetration test information sources include systems, appliances, devices, services, and applications (including databases).
(c) CCIC directed penetration test information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.5 – When selected, penetration testing on a production system must be conducted in a manner that minimized risk of information corruption or service outage.
Std.6 – When selected, raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Supplemental Guidance:

Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems will have against adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of internal and external adversaries in carrying out hostile cyber-attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.

External penetration testing attempts to duplicate the actions of external adversaries (outside the security perimeter) in carrying out hostile cyber-attacks against the organization. Internal penetration testing is performed from inside the system security perimeter.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC

upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When user session information and other PII is captured or recorded during penetration testing, ensure relevant privacy controls are addressed.

Reference(s): Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; NIST SP: 800-115; OMB Memo: M-14-03, M-15-01, M-16-04; OMB Circular A-130: 7.g. and 8.b(3)	**Related Controls Requirement(s):** AP-1, AP-2, SA-12, TR-1, TR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; procedures addressing penetration testing; system security plan; security assessment report; security assessment evidence; penetration test 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 penetration testing responsibilities.
Penetration test results must be made available to the CMS Cybersecurity Integration Center (CCIC) for review, aggregation, and analysis at the enterprise level.

CA-9	Internal System Connections (High, Moderate, Low)	Assurance	P2

Control:

The organization:
a. Authorizes connections of defined internal information system components or classes of components (defined in the applicable system 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.

Implementation Standards:

High & Moderate:

Std.1 - The security plan will identify the types of personally owned equipment that may be internally connected with organizational information systems and networks:
- Compliant with CMS and HHS policies on use of personally owned equipment
- Use of Bluetooth interconnections is disallowed without explicit approval of the Authorizing Official (AO).

Supplemental 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, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Include privacy requirements in the Information Connection Document (or equivalent such as an Interconnection Security Agreement or an Authority to Connect package), specifically addressing the collection authority, compatibility of purpose for use, and need for recipient of information to achieve specific business purpose. Documentation must also address responsibilities of the receiving information system for protecting personally identifiable information (PII).

Reference(s): Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; HHS: Information Systems Security and Privacy Policy (IS2P) 2014; OMB Circular A-130: 7.g. and 8.b(3)(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1)	**Related Controls Requirement(s):** AC-3, AC-4, AC-18, AC- 19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4, UL-1, UL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; access control policy; procedures addressing information system connections; system 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; plan of action and milestones; information system monitoring records; security impact analyses; status reports; and other relevant documents or records.
Interview: Organizational personnel with component connection authorization responsibilities.

CA-9(1)	Non-Mandatory: Security Compliance Checks	P3

Control:

The information system performs security compliance checks, as defined by the RMH, on constituent system components prior to the establishment of the internal connection.

Supplemental Guidance:

Security compliance checks may include, for example, verification of the relevant baseline configuration.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Security compliance checks may include an assessment, prior to initial connection, of specific components, e.g., printers, based on sensitivity of personally identifiable information (PII) processed by that component. Any change to the components' security posture would require a re-verification of the configuration settings.

Reference(s): Code: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130: 7.g. and 8.b(3)(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.306(a); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1)	**Related Controls Requirement(s):** CM-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the information system performs security compliance checks on constituent system components prior to the establishment of the internal connection.

Assessment Methods and Objects:

Examine: Security assessment and authorization policy; access control policy; procedures addressing information system connections; system 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; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with component connection authorization responsibilities.

B.5 Configuration Management (CM)

CM-1	Configuration Management Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

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

Implementation Standards:

High, Moderate, & Low:

Std.1 - The configuration management process and procedure is documented to define configuration items at the system and component level (e.g., hardware, software, workstation); monitor configurations; and 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, replacement of critical hardware components).

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, AS-3, CM-1, SM-1, SM-3; NIST SP: 800-12, 800-100	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy and procedures; other relevant documents or records.
Interview: Organizational personnel with configuration management and control responsibilities.

CM-2	Baseline Configuration (High, Moderate, Low)	Assurance	P1

Control:

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Implementation Standards:

High, Moderate, & Low:

Std.1 – Baseline configurations will be distilled from government, industry, and vendor standards and best practices.
Std.2 – Baseline configurations must include security updates.
Std.3 – Baseline configuration requirements apply to all systems, devices, appliances, and applications.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-2; HHS: End of Life Operating Systems and Applications Policy; NIST SP: 800-128	**Related Controls Requirement(s):** CM-3, CM-6, CM-8, CM-9, PM-5, PM-7, SA-10

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; and other relevant documents or records.
Examine: Information system is configured to defined baseline configuration, and the baseline configuration documentation is kept up-to-date.
Examine: Baseline configurations include implementation of government, industry, and vendor standards and best practices.

CM-2(1)	Reviews and Updates (High, Moderate)	Assurance	P1

Control:

The organization reviews and updates the baseline configuration of the information system:
a. At least every 180 days for High systems or 365 days for Moderate systems;
b. When configuration settings change due to critical security patches (as defined by the Federal Government, CMS, or vendor), upgrades and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), major system changes/upgrades;
c. As an integral part of:
1. information system component installations;
2. upgrades; and
3. updates to applicable governing standards (implemented within timeline defined in (a) above); and
d. Supporting baseline configuration documentation reflects ongoing implementation of operational baseline configuration updates, either directly or by policy.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization reviews and updates the baseline configuration of the information system: (a) At least every 365 days; (b) When required due to a significant change; and (c) As an integral part of information system component installations and upgrades.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-128	**Related Controls Requirement(s):** CM-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

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; and other relevant documents or records.
Interview: Organizational personnel with configuration change control responsibilities.

CM-2(2)	Automation Support for Accuracy/Currency (High)	Assurance	P1

Control:

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Supplemental Guidance:

Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM- 8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities.

Reference(s): FedRAMP Rev. 4 Baseline; Office of Management and Budget (OMB): M-14-03, M-15-01; NIST SP: 800-37, 800-100, 800-128	**Related Controls Requirement(s):** CM-7, RA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; and other relevant documents or records.
Test: Automated mechanisms implementing baseline configuration maintenance.

CM-2(3)	Retention of Previous Configurations (High, Moderate)	Assurance	P1

Control:

The organization retains older versions of baseline configurations of the information system as deemed necessary to support rollback.

Implementation Standards:

High & Moderate:

Std.1 – Following baseline configuration updates, no less than one (1) older baseline configuration must be maintained (e.g., for emergency rollback).

Supplemental Guidance:

Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-34, 800-100, 800-128	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; historical copies of baseline configurations; and other relevant documents or records.

CM-2(6)	Non-Mandatory: Development and Test Environments	Assurance	P3

Control:

The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration.

Implementation Standards:

High:

Std.1 - The organization must provide separated environments where execution and analysis of data may present an enhanced risk to the system.

Supplemental Guidance:

Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments.

Reference(s): NIST SP: 800-128	**Related Controls Requirement(s):** CM-4, SC-3, SC-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; and other relevant documents or records.
Test: Automated mechanisms implementing baseline configuration environments.

CM-2(7)	Configure Systems, Components, or Devices for High-Risk Areas (High, Moderate)	Assurance	P1

Control:

The organization:

a. Issues dedicated information systems, system components, or devices with stringent configurations (e.g., FIPS 140-2 for encryption) to individuals traveling to locations that the organization deems to be of significant risk; and
b. Applies security safeguards to the devices (i.e., detailed inspection of the device for physical tampering, purging or reimaging the hard disk drive/removable media) when the individuals return.

Supplemental Guidance:

When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the Media Protection (MP) family.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-128	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Interview: Organizational personnel with configuration change control responsibilities.

CM-3	Configuration Change Control (High, Moderate)	Assurance	P1

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 a minimum of three (3) years after the change;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through change request forms which must be approved by an organizational and/or CMS change control board that convenes frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization coordinates and provides oversight for configuration change control activities through organization-defined configuration change control element (via, e.g., a committee or board) that convenes at an organization-defined frequency; and, the organizations maintain organization-defined frequency; organization-defined configuration change conditions.
CSP.2 - For CSPs, the organization defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the Joint Authorization Board (JAB).
CSP.3 - For CSPs, the organization establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the Federal Government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3, CM-6; NIST SP: 800-128; 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(e)(2)(ii)	**Related Controls Requirement(s):** CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system architecture and configuration documentation; system security plan; change control records; information system audit records; and other relevant documents or records.
Examine: Organization facilitates required oversight of privacy reporting by CMS (including coordination and cooperation with the CMS Cybersecurity Infrastructure Center [CCIC]).
Interview: Organizational personnel with configuration change control responsibilities.

CM-3(1)	Automated Document/Notification/Prohibition of Changes (High)	Assurance	P1

Control:

The organization employs automated mechanisms to:
a. Document proposed changes to the information system;
b. Notify designated approval authorities (defined in the applicable security plan) of proposed changes to the information system;
c. Request change approval per the system configuration management documentation;
d. Highlight proposed changes that have been waiting an approval decision, or have not been approved, for longer than change management procedure (defined in the applicable security plan) requires;
e. Prohibit changes to the information system until approvals are received;
f. Document all changes to the information system; and
g. Notify stakeholders when approved changes are completed.
A list of potential stakeholders must include, but is not limited to the following:
a. Change Control Board (CCB);
b. Configuration Management Executive;
c. Chief Risk Officer (CRO);
d. Cyber Risk Advisor (CRA);
e. ISSO;
f. Program Manager;
g. Data Guardian;
h. Information System Owner (ISO); and
i. Information System Administrator.

Supplemental Guidance:

None.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; automated configuration control mechanisms; change control records; information system audit records; and other relevant documents or records.
Test: Automated mechanisms implementing configuration change control.

CM-3(2)	Test/Validate/Document Changes (High, Moderate)	Assurance	P1

Control:

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Supplemental 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 procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with 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).
- To better secure IT infrastructure, configuration management procedure should include use of a security configuration checklist (sometimes called a lockdown, hardening guide, or benchmark) to help configure systems to an operating environment.
- Security authorization (authorization to operate given identified risk and security controls) is maintained when proposed or actual changes to the information system, and their suspected impact on the security of the system, are documented and continuously monitored for compliance.
- Configuration Management process includes the following steps:
1. Identify change;
2. Evaluate change request;
3. Approve, Deny or Defer implementation of the change;
4. Implement the approved change; and
5. Continuously monitor change for acceptable operation.

Reference(s): NIST SP: 800-100	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; change control records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with configuration change control responsibilities.

CM-3(6)	Non-Mandatory: Cryptography Management	P3

Control:

The organization ensures that all cryptographic mechanisms used to provide protection to sensitive information are under configuration management.

Supplemental Guidance:

Regardless of the cryptographic means employed (e.g., public key, private key, shared secrets), organizations ensure that there are processes and procedures in place to effectively manage those means. For example, if devices use certificates as a basis for identification and authentication, there needs to be a process in place to address the expiration of those certificates.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When encrypting personally identifiable information (PII), management processes must be in place to ensure future access to such data.

Guidance for systems processing, storing, or transmitting PHI:

When encrypting PHI, there must be management processes in place to ensure future access to such data.

Reference(s):	**Related Controls Requirement(s):** SC-8, SC-12, SC-13, SC- 28

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization:
(i) defines security safeguards provided by cryptographic mechanisms that are to be under configuration management; and
(ii) ensures that cryptographic mechanisms used to provide organization-defined security safeguards are under configuration management.

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; change control records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with configuration change control responsibilities.

CM-4	Security Impact Analysis (High, Moderate, Low)	Assurance	P2

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.

Supplemental Guidance:

Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers [ISSO], 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When analyzing changes to the information system, the impacts to privacy are also considered. If necessary, conduct a privacy impact assessment.

Reference(s): E-Government Act of 2002 (Pub. L. No. 107-347), §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-4; NIST SP: 800-128; OMB Memo: M-03-22; 45 C.F.R. §164.308(a)(1)(ii)(A); 45 C.F.R. §164.308(a)(1)(ii)(B); 45 C.F.R. §164.308(a)(8)	**Related Controls Requirement(s):** AR-2, CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 architecture and configuration documentation; change control records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for determining security and privacy impacts prior to implementation of information system changes.

CM-4(1)	Separate Test Environments (High)	Assurance	P2

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.

Supplemental 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).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

If personally identifiable information (PII) is used in the test environment, then the same controls required for systems containing PII must be applied to the test environment. Simulated PII information should be used to the maximum extent practicable when testing system functionality.

Reference(s): Code: 5 U.S.C. §552a(e)(10); OMB Circular A-130: 7.g.	**Related Controls Requirement(s):** AP-2, AR-3, DM-2, DM-3, SA-11, SA-15(9), SC-3, SC-7, UL-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; information system test and operational environments; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.

CM-4(2)	Non-Mandatory: Verification of Security Functions	Assurance	P3

Control:

The organization must ensure changes in information system security functions are verified:
a. To be implemented per approved design;
b. To integrate and operate as intended; and
c. To produce expected results.

Implementation Standards:

High & Moderate:

Std.1 - Any system, including development and test, that contains and/or processes sensitive information (e.g., personally identifiable information [PII]) must verify security functions as per this control.
Std.2 - The system's security functions must be continuously monitored and evaluated to ensure they are operating as intended and changes do not have an adverse effect on system performance.
Std.3 - Actions must be taken to verify that the provisioned security function implementation being assessed and/or monitored meets security function requirements, and is an approved system configuration.

Supplemental Guidance:

Implementation in this context refers to installing changed code in the operational information system.
In general, the goal is to verify that system changes do not adversely impact security functions and the system's ability to meet mission requirements.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

If a system change is made, verification of Privacy Overlay security control functions is required to ensure continued compliance with privacy-related statutes and regulations.

Reference(s): Code: 5 U.S.C. §552a(e)(10); OMB Circular A-130: 7.g.; 45 C.F.R. §164.308(a)(7)(ii)(D); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(2)(iii)	**Related Controls Requirement(s):** SA-11

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; change control records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.

CM-5	Access Restrictions for Change (High, Moderate)	P1

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 must be generated, reviewed, and retained.

Supplemental 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).

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-4; NIST SP: 800-100	**Related Controls Requirement(s):** AC-3, AC-6, PE-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities.
Test: Change control process and associated restrictions for changes to the information system.

CM-5(1)	Automated Access Enforcement/Auditing (High)	P1

Control:

The information system enforces access restrictions and supports auditing of the enforcement actions.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (CM-5(1) CSP.1) as a replacement for the above Control Enhancement (CM-5(1)). The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

Supplemental Guidance:

Organizations log access records associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-100	**Related Controls Requirement(s):** AU-2, AU-6, AU-12, CM-3, CM-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

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; change control records; information system audit records; and other relevant documents or records.
Test: Mechanisms implementing access restrictions for changes to the information system.

CM-5(2)	Review System Changes (High)	P1

Control:

The organization reviews information system changes:
a. At least once a week; and
b. When unauthorized changes or unexpected levels of system performance are indicated.

Implementation Standards:

High:

Std.1 - The system configuration must be continuously monitored as a supplemental information source for the review processes.
Std.2 - Information system changes must be verified to meet system mission and user requirements.

Supplemental Guidance:

Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process.
The results of the review include evidence of control effectiveness and recommendations for correcting any deficiencies are documented.

Reference(s): NIST SP: 800-37, 800-100	**Related Controls Requirement(s):** AU-6, AU-7, CM-3, CM-5, PE-6, PE-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; system security plan; change control records; information system audit records; and other relevant documents or records

CM-5(3)	Signed Components (High)	P1

Control:

The information system prevents the installation of network and server software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Supplemental Guidance:

Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. The use of digital signatures, in conjunction with organizational verification of such signatures, is a method of code authentication.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** CM-7, SC-13, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; list of critical software programs to be prohibited from installation without an approved certificate; information system design documentation; information system architecture and configuration documentation; system security plan; change control records; information system audit records; and other relevant documents or records.
Test: Information system mechanisms preventing installation of software programs not signed with an organization-approved certificate. Self-signed certificates are disallowed.

CM-6	Configuration Settings (High, Moderate, Low)	P1

Control:

The organization:
a. Establishes and documents configuration settings for information technology products employed within the information system using the latest security baseline configurations established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 (refer to Implementation Standard 1 for specifics) that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements (defined in the applicable system security plan); and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Use of HHS and CMS approved Operating System (OS)
(a) HHS-specific minimum security configurations must be used for the following OS and Applications:
1. HHS approved USGCB Windows Standards (e.g., Microsoft supported versions only); and
2. Blackberry Server - Websense.
(b) For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is:
1. USGCB;
2. NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order;
3. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG);
4. National Security Agency (NSA) STIGs;
5. 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.
6. In situations where no guidance exists, coordinate with CMS for guidance. CMS must collaborate within CMS and the HHS Cybersecurity Program, and other organizations through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to:
- Establish baseline configurations and communicate industry and vendor best practices; and
- Ensure deployed configurations are supported for security updates.
7. All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented.

Systems defined as CSPs:

High & Moderate, & Low:

CSP.1 - For CSPs, the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using USGCB that reflect the most restrictive mode consistent with operational requirements.
CSP.2 - For CSPs, the organization must use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establish own configuration settings if USGCB is not available. Configuration settings are approved and accepted by the Joint Authorization Board (JAB).
CSP.3 - For CSPs, the organization ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).

Supplemental Guidance:

Configuration settings are the set 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, 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, 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, and 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 each system's baseline configuration.
Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, 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 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.
Legacy operating systems without ongoing vendor support, such as Windows XP or older desktop OS, Windows Server 2003 or older server OS, Solaris 9 or older OS, or Red Hat Linux 9 or older, are only permissible if documented within the Risk Assessment and System Security Plan and authorized by the Authorizing Official (AO).

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-2; HHS: End of Life Operating Systems and Applications Policy; NIST SP: 800-70, 800-128; OMB Memo: M-07-18, M-08-22; Web: checklists.nist.gov, nsa.gov, nvd.nist.gov	**Related Controls Requirement(s):** AC-19, CM-2, CM-3, CM- 7, CM-8, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; system security plan; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records.
Examine: Information systems are configured to baseline configurations:
- Only approved operating systems are found;
- Only approved deviations are found; and
- Monitors configuration on a regular basis.

Interview: Organizational personnel with security configuration responsibilities.

CM-6(1)	Automated Central Management/Application/Verification (High)	P1

Control:

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for information system components as defined in the HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications.

Implementation Standards:

High:

Std.1 - The system must be continuously monitored and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance.
Std.2 - Information system automated central management systems must be verified to meet system mission and user requirements.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-100; HHS: Minimum Security Configuration Standards for Departmental Operating Systems and Applications	**Related Controls Requirement(s):** CA-7, CM-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records. **Test:** Automated mechanisms implementing the centralized management, application, and verification of configuration settings.

CM-6(2)	Respond to Unauthorized Changes (High)	P1

Control:

The organization responds to unauthorized changes to information system and components (e.g., authorization, auditing, processing types, baseline configurations) and data (e.g., system libraries, log files, executables) in the following ways:
a. Alert responsible actors (person, organization);
b. Restore to approved configuration; and
c. Halt system processing as warranted.

Supplemental Guidance:

Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in the extreme case, halting affected information system processing.

Guidance for systems defined as CSPs:

Information on the US Government Configuration Baseline (USGCB) checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc.

Reference(s): NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** IR-4, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; system security plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records.
Test: Automated mechanisms implementing responses to unauthorized changes to configuration settings.

CM-7	Least Functionality (High, Moderate, Low)	P1

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.
c. A list of specifically needed system services, ports, and network protocols must be maintained and documented in the applicable security plan; all others will be disabled.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Automated configuration review results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Configuration review information sources include systems, appliances, devices, services, and applications (including databases).
(c) CCIC directed configuration review information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.
Std.3 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational configuration status and posture information.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - CSPs must implement this Standard (CM-7 CSP.1) as a replacement for the above Control (CM-7). 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: USGCB-defined list of prohibited or restricted functions, ports, protocols, and/or services.
CSP.2 - For CSPs, the organization must 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. The list of prohibited or restricted functions, ports, protocols, and/or services are approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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). Additionally, 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., VoIP, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., USB, FTP, and Hypertext Transfer Protocol [HTTP]) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and 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.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Guidance for systems defined as CSPs:

Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	Related Controls Requirement(s): AC-6, CM-2, RA-5, SA-5, SC-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records.
Examine: Information systems are configured to provide only the functionality necessary to perform mission. Examples:
1. Networking minimizes functionality;
2. Privileged escalation mechanisms (tools) are properly configured;
3. Applications, including network protocols, are configured to maximize security; and
4. Firewall rules follow deny-all, permit-by-exception policy.
Examine: Information systems provide the capability to detect changes in configurations in an automated manner.
Test: Information system for disabling or restricting functions, ports, protocols, and services.

CM-7(1)	Periodic Review (High, Moderate)	P1

Control:

The organization:
(a) Reviews the information system no less often than once every thirty (30) days to identify and eliminate unnecessary functions, ports, protocols, and/or services;
(b) Performs automated reviews of the information system no less often than once every seventy-two (72) hours to identify changes in functions, ports, protocols, and/or services; and
(c) Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

Implementation Standards:

High & Moderate:

Std.1 - Periodic configuration review results that are generated by automated tools must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Configuration review information sources include systems, appliances, devices, services, and applications (including databases); and
(c) CCIC directed configuration automated periodic review information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (CM-7(1) CSP.1) as a replacement for the previous Implementation Standards for this Control(CM-7(1) Std.1 and Std.2). The organization reviews the information system no less often than quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Supplemental Guidance:

The organization can either determine 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.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M- 16-04	**Related Controls Requirement(s):** AC-18, CM-7, IA-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records.
Examine: Information system provides the capability to identify changes in configurations in an automated manner.
Interview: Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the information system.

CM-7(2)	Prevent Program Execution (High, Moderate)	P1

Control:

The information system prevents program execution in accordance with policies regarding authorized software use which include, but are not limited to the following:
a. Software must be legally licensed;
b. Software must be provisioned in approved configurations; and
c. Users must be authorized for software program use.

Supplemental Guidance:

This control enhancement addresses organizational policies restricting software usage as well as the terms and conditions imposed by the developer or manufacturer including, for example, software licensing and copyrights. Restrictions include, for example, restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** CM-8, PM-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; and other relevant documents or records.
Test: Automated mechanisms preventing software program execution on the information system

CM-7(5)	Authorized Software/Whitelisting (High)	P1

Control:

The organization:
a. Identifies defined software programs (defined in the applicable security plan) authorized to execute on the information system;
b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system;
c. Reviews and updates the list of authorized software programs no less often than every seventy-two (72) hours; and
d. Receives automated updates from a trusted source.

Systems defined as CSPs:

High & Moderate

The organization:
a. Identifies defined software programs (defined in the applicable security plan) authorized to execute on the information system;
b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system;
c. Reviews and updates the list of authorized software programs no less often than every seventy-two (72) hours; and
d. Receives automated updates from a trusted source.

Implementation Standards:

High:

Std.1 - An automated software whitelisting tool must be implemented.
Std.2 - Authorized software whitelisting results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Authorized software whitelisting (and blacklisting) information sources include systems, appliances, devices, services, and applications (including databases);
(c) Authorized software whitelisting information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and
(d) CCIC directed unauthorized software/whitelisting information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Systems defined as CSPs:

High & Moderate:

CSP.1 - Automated authorized software/whitelisting tool results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Continuous Diagnostics and Mitigation requirements;
(b) Authorized software/whitelisting (and blacklisting) information sources include systems, appliances, devices, services, and applications (including databases);
(c) Authorized software/whitelisting information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and
(d) CCIC directed unauthorized software/whitelisting information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
CSP.2 - As required by CMS, raw security information/results from relevant automated tools must be provided unaltered to the CCIC.

Supplemental Guidance:

The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup.
Control enhancement CM-7(5) is only required for systems categorized under FIPS-199 as HIGH. Implementation of whitelisting is an option for all systems (e.g., to include any system categorized under FIPS-199 as MODERATE and LOW). If the system owner/business owner chooses to implement CM-7(5) on systems categorized under FIPS-199 as MODERATE and LOW, CM-7(4) does not have to be implemented.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M- 16-04	**Related Controls Requirement(s):** CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; and other relevant documents or records.
Interview: Organizational personnel with information security responsibilities; system/network administrators.
Test: Automated mechanisms preventing software program execution on the information system.

Systems defined as CSPs:

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system design documentation; specifications relevant to preventing software program execution; information system configuration settings and associated documentation; and other relevant documents or records.
Interview: Organizational personnel with information security responsibilities; system/network administrators.
Test: Automated mechanisms preventing software program execution on the information system.

CM-8	Information System Component Inventory (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops and documents an inventory of information system components that:
1. Accurately reflects the current information system;
2. Include all components within the authorization boundary of the information system;
3. Are at the level of granularity deemed necessary for tracking and reporting; and
4. Includes:
- Each component's unique identifier and/or serial number;
- Information system of which the component is a part;
- Type of information system component (e.g., server, desktop, application);
- Manufacturer/model information;
- Operating system type and version/service pack level;
- Presence of virtual machines;
- Application software version/license information;
- Physical location (e.g., building/room number);
- Logical location (e.g., IP address, position with the information system [IS] architecture);
- Media access control (MAC) address;
- Ownership;
- Operational status;
- Primary and secondary administrators; and
- Primary user.

b. Reviews and updates the information system component inventory no less frequently than every 180 days for High systems or 365 days for Moderate and Low systems, or per CM-8(1) and/or CM-8(2), as applicable.

Implementation Standards:

High, Moderate, & Low:

Std.1 - All Government-owned equipment (i.e., servers, workstations, laptops, and other IT components) used to process, store, or transmit CMS information display an asset tag with a unique identifying asset number.
Std.2 - IT components with an asset tag are tracked in an asset inventory database to include (at a minimum) name of component, location, asset identification, owner, and description of use.
Std.3 - Fully integrate inventory of information system components with the organizational continuous monitoring capability (CM-7).
Std.4 - Automated asset inventory information tracking systems must:
(a) Transmit updates to CCIC no less often that once every 72 hours.
Std.5 - Automated component tracking and management tool results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Authorized component information sources include systems, platforms, appliances, devices;
(c) Component information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and
(d) CCIC directed authorized component information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.6 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.
Std.7 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational component status and posture information.
Std.8 - The organization must create and maintain the inventory of high value assets associated with the system.
(a) The inventory must identify other FISMA systems from which controls are inherited.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization develops, documents, and maintains an inventory of information system components that includes organization-defined information deemed necessary to achieve effective property accountability.
CSP.2 - For CSPs, the organization defines information deemed necessary to achieve effective property accountability. Property accountability information are approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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, 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, 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.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Guidance for systems defined as CSPs:

Information deemed necessary to achieve effective property accountability may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-2; HIPAA: 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(iii); NIST SP: 800-37, 800-39, 800-128, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** CM-2, CM-6, PM-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; system security plan; information system inventory records; and other relevant documents or records.
Examine: Information systems and components managed within organizational automated inventory management capability.
Test: Organizational processes for updating inventory of information system components; automated mechanisms implementing updating of the information system component inventory.

CM-8(1)	Updates During Installations/ Removals (High, Moderate)	Assurance	P1

Control:

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Supplemental Guidance:

No generic guidance.

Guidance for systems processing, storing, or transmitting PHI:

Identifying any changes or updates to system inventories allows organizations to accurately track the equipment on which their information systems are run and to maintain an accurate inventory of hardware and software used to collect and manage PHI. Maintaining a current inventory supports accountability controls and may also support breach response efforts.

Guidance for systems defined as CSPs:

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 an 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.

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; and other relevant documents or records.
Interview: Organizational personnel with information system installation and inventory responsibilities.

CM-8(2)	Automated Maintenance (High)	P1

Control:

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Supplemental Guidance:

Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine information system component inventory and baseline configuration activities.

Reference(s): OMB Memo: M-16-04	**Related Controls Requirement(s):** SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; and other relevant documents or records.
Test: Automated mechanisms implementing information system component inventory management.

CM-8(3)	Automated Unauthorized Component Detection (High, Moderate)	Assurance	P1

Control:

The organization:
a. Employs automated mechanisms 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 and/or provisioned configurations are detected:
1. Disable access to the identified component;
2. Disable the identified component's network access;
3. Isolate the identified component; and
4. Notify the responsible actor (i.e., person/organization-defined in security plan).

Implementation Standards:

High & Moderate:

Std.1 - All components within the system authorization boundary must be monitored in compliance with information security continuous monitoring (ISCM) requirements.

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (CM-8(3) CSP.1) as a replacement for the above Control Enhancement (CM-8(3)). The organization:
(a) Employs automated mechanisms to scan continuously, using automated mechanisms with a maximum five-minute delay in detection to detect the addition of unauthorized components/devices into the information system; and
(b) Disables network access by such components/devices or notifies designated organizational officials.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AC-17, AC-18, AC-19, CA-7, CM-8, RA-5, SI-3, SI-4, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; system security plan; information system design documentation; information system inventory records; component installation records; change control records; and other relevant documents or records.
Test: Automated mechanisms for detecting unauthorized components/devices on the information system.

CM-8(4)	Accountability Information (High)	Assurance	P1

Control:

The organization includes in the information system component inventory information, a means for identifying by position and role, and individuals responsible/accountable for administering those components.

Supplemental Guidance:

Identifying individuals who are both responsible and accountable for administering information system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required (e.g., component is determined to be the source of a breach or compromise, component needs to be recalled/replaced, or component needs to be relocated).

Reference(s): OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; and other relevant documents or records.

CM-8(5)	No Duplicate Accounting of Components (High, Moderate)	Assurance	P1

Control:

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

Supplemental Guidance:

This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; system security plan; information system inventory records; component installation records; and 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.

CM-9	Configuration Management Plan (High, Moderate)	Assurance	P1

Control:

The organization develops, documents, and implements a configuration management plan for the information system that:
a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying and managing configuration items throughout the system development life cycle;
c. Defines the configuration items for the information system;
d. Places the configuration items under configuration management; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

Supplemental 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 how configuration management is used 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 baseline configurations, 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.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-128	**Related Controls Requirement(s):** CM-2, CM-3, CM-4, CM-5, CM-8, SA-10

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Configuration management policy; configuration management plan; procedures addressing configuration management planning; system security plan; and other relevant documents or records.

CM-10	Software Usage Restrictions (High, Moderate, Low)	P2

Control:

The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AC-17, CM-8, SC-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Software use policy, contract agreements, site licenses, software installation policy and procedures, file sharing policy, security plan; and other relevant documents or records.
Interview: 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.

CM-11	User-Installed Software (High, Moderate, Low)	P1

Control:

The organization:
a. Prohibits the installation of software by users on all GFE;
b. Enforces software installation policies through organization-defined methods (defined in the applicable security plan); and
c. Monitors policy compliance at least monthly.

Implementation Standards:

High:

Std.1 - Monitoring for user-installed software must comply with information security continuous monitoring (ISCM) requirements.
Std.2 - Whitelisting applications must prevent un-authorized user-installed software.

Moderate & Low:

Std.1 - Monitoring for user-installed software must comply with information security continuous monitoring (ISCM) requirements.

Supplemental Guidance:

If provided the necessary privileges, users can 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. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Software use policy, contract agreements, site licenses, software installation policy and procedures, file sharing policy, security plan; and other relevant documents or records.

B.6 Contingency Planning (CP)

CP-1	Contingency Planning Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

b. Reviews and updates (as necessary) the current:

1. Contingency planning policy at least every three (3) years or as necessitated by significant change.
2. Contingency planning procedures at least every three (3) years or as necessitated by significant change.

Supplemental 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Contingency planning policy and procedures must take privacy-applicable requirements into account so that executing contingency measures does not result in avoidable privacy incidents and breaches.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(7)(i); NIST SP: 800-12, 800-34, 800-100	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with contingency planning responsibilities.

CP-2	Contingency Plan (High, Moderate, Low)	P1

Control:

The organization:

a. Develops a contingency plan for the information system in accordance with NIST SP 800-34 that:

1. Identifies essential CMS missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles and responsibilities, and assigns these to specific individuals with contact information;
4. Addresses maintaining essential CMS 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 ISSO, Business Owner, Contingency Plan Coordinator (CPC), and other stakeholders identified within the contingency plan;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system within every three hundred sixty-five (365) days;

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to key contingency personnel, system administrator, database administrator, and other personnel/roles as appropriate and organizational elements identified above; and
g. Protects the contingency plan from unauthorized disclosure and modification.

Implementation Standards:

High, Moderate, & Low:

Std.1 - The system must be continuously monitored and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance.

Std.2 - The organization must verify that the provisioned implementation being assessed and/or monitored meets users' needs and is an approved system configuration.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom the organization will distribute the CP. The contingency list includes designated FedRAMP personnel.

CSP.2 - For CSPs, the organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom the organization will communicate any CP changes. The contingency list includes designated FedRAMP personnel.

Supplemental 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 impacted. 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Contingency plans must take privacy-applicable requirements into account so that executing contingency measures does not result in avoidable privacy incidents and breaches.

Guidance for systems processing, storing, or transmitting PHI:

The contingency plan for systems containing PHI must include:

1) Data backup plan,
2) Disaster recovery plan,
3) Emergency mode operation plan, and
4) Emergency access procedures.

Additionally, the decision to include the following is dependent on a risk analysis to determine if or to what extent these should be included in the contingency plan:

1) Testing and revision procedures,
2) Applications and data criticality analysis, and
3) Contingency operations (i.e., procedures that allow facility access in support of restoration of lost data.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-3; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(C), 45 C.F.R. §164.308(a)(7)(ii)(E), 45 C.F.R. §164.308(a)(7)(i)-(ii); 45 C.F.R. §164.310(a)(2)(i);	**Related Controls 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

45 C.F.R. §164.312(a)(2)(ii); Homeland Security Presidential Directive (HSPD) 7: G(22)(i); NIST SP: 800-34;	

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; and other relevant documents or records.
Examine: CFACTS to ensure contingency contact information is being maintained.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities.

CP-2(1)	Coordinate with Related Plans (High, Moderate)	P1

Control:

The organization coordinates contingency plan development with organizational elements responsible for related plans.

Supplemental Guidance:

Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans (COOP), Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

Reference(s): FedRAMP Rev. 4 Baseline; HSPD 7: G(22)(i); NIST SP: 800-34	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas.

CP-2(2)	Capacity Planning (High)	P1

Control:

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Supplemental Guidance:

Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber-attacks) can result in a reduction of 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.

Reference(s): FedRAMP Rev. 4 Baseline; HSPD 7: G(22)(i); NIST SP: 800-34	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-2(3)	Resume Essential Missions/Business Functions (High, Moderate)	P1

Control:

The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.

Supplemental 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 for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-34	**Related Controls Requirement(s):** PE-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; business impact assessment; other related plans; and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-2(4)	Resume All Missions/Business Functions (High)	

Control:

The organization plans for the resumption of all missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.

Supplemental 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 period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.

Reference(s): NIST SP: 800-34	**Related Controls Requirement(s):** PE-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; business impact assessment; other related plans; and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-2(5)	Continue Essential Missions/Business Functions (High)	P1

Control:

The organization plans for the continuance of Primary Mission Essential Functions (PMEF) with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

Supplemental 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. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites).

Guidance for systems processing, storing, or transmitting PHI:

Pursuant to the emergency mode operations plan and emergency access procedure mandated under HIPAA, this control is required for both provision of emergency services (a mission critical business function), and for protection of the security of PHI while operating in emergency mode.

Reference(s): NIST SP: 800-34; 45 C.F.R. §164.308(a)(7)(ii)(C); 45 C.F.R. §164.312(a)(2)(ii)	**Related Controls Requirement(s):** PE-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; business impact assessment; other related plans; and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-2(8)	Identify Critical Assets (High, Moderate)	P1

Control:

The organization identifies information system assets supporting essential missions and business functions.

Supplemental 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 so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted 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 aid in identifying critical assets.

Guidance for systems processing, storing, or transmitting PHI:

This control addresses the HIPAA Security Rule requirement to assess the relative criticality of specific applications and data to facilitate a risk-based contingency plan. Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-34, 800-60; 45 C.F.R. §164.308(a)(7)(ii)€	**Related Controls Requirement(s):** SA-14, SA-15

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; business impact assessment; other related plans; and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-3	Contingency Training (High, Moderate, Low)	Assurance	P2

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.

Supplemental Guidance:

Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. 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 confirm that appropriate training has been completed.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); NIST SP: 800-16, 800-50	**Related Controls Requirement(s):** AT-2, AT-3, CP-2, IR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; system security plan; contingency training records; and other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-3(1)	Simulated Events (High)	Assurance	P2

Control:

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Supplemental Guidance:

None.

Reference(s): HSPD 7: G(22)(i)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; and other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-4	Contingency Plan Testing (High, Moderate, Low)	Assurance	P2

Control:

The organization:
a. Tests the contingency plan for the information system within every three hundred sixty-five (365) days using NIST (NIST SP 800-34, NIST SP 800-84) and CMS -defined tests and exercises, such as tabletop tests, in accordance with the current CMS contingency plan procedure to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Systems defined as CSPs:

The organization:
a. Tests the contingency plan for the information system within every three hundred sixty-five (365) days using NIST or CMS -defined tests and exercises, such as tabletop tests, in accordance with the current CMS contingency plan procedure to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - Contingency plan test results will be made available to the CMS business owner and all system developers and maintainers deployed within the CSP environment.
CSP.2 - For CSPs, the organization tests and/or exercises the contingency plan for the information system at least every 365 days using functional exercises to determine the plan's effectiveness and the organization's readiness to execute the plan.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PHI:

Contingency plan tests and exercises should include an evaluation of the ability to meet privacy requirements in a contingency scenario as well as corrective measures to address any privacy risks identified.
Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s):	**Related Controls Requirement(s):** CP-2, CP-3, IR-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; system security plan; contingency plan testing and/or exercise documentation; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises.

CP-4(1)	Coordinate with Related Plans (High, Moderate)	P2

Control:

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Implementation Standards:

High & Moderate:

Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope:
1. Continuity of Operations Plan (COOP)
2. Business Continuity Plan (BCP)
3. Critical Infrastructure Protection (CIP) Plan
4. Disaster Recovery Plan (DRP)
5. Information System Contingency Plan (ISCP)
6. Cyber Incident Response Plan
7. Occupant Emergency Plan (OEP)

Supplemental Guidance:

Plans related to contingency plans for organizational information systems include, for example, BCPs, DRPs, COOPs, Crisis Communications Plans, Critical Infrastructure Protect (CIP) Plans, Cyber Incident Response Plans, and OEPs. 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.

Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope:
1. COOP
2. BCP
3. CIP Plan
4. DRP
5. ISCP
6. Cyber Incident Response Plan
7. OEP

Reference(s): FedRAMP Rev. 4 Baseline; HSPD 7: G(22)(i); NIST SP: 800-34	Related Controls Requirement(s): IR-8, PM-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; and other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; and organizational personnel with responsibilities for related plans.

CP-4(2)	Alternate Processing Site (High)	P2

Control:

The organization tests the contingency plan at the alternate processing site:
a. To familiarize contingency personnel with the facility and available resources; and
b. To evaluate the capabilities of the alternate processing site to support contingency operations.

Supplemental Guidance:

None.

Reference(s): HSPD 7: G(22)(i)	Related Controls Requirement(s): CP-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; and other relevant documents or records.

CP-4(4)	Non-Mandatory: Full Recovery/Reconstitution	P3

Control:

The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Supplemental Guidance:

This control enhancement is highly recommended for any system designated as a High Value Asset (HVA)

Reference(s):	Related Controls Requirement(s): CP-10, SC-24

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan testing and/or exercise documentation; contingency plan test results; and other relevant documents or records.
Interview: Organizational personnel with information system recovery and reconstitution responsibilities; and organizational personnel with contingency plan testing and/or exercise responsibilities.

CP-6	Alternate Storage Site (High, Moderate)	P1

Control:

The organization:
a. Establishes an alternate storage site, including 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.

Supplemental 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 if 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(a)(2)(i); NIST SP: 800-34	**Related Controls Requirement(s):** CP-2, CP-7, CP-9, CP-10, MP-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; and other relevant documents or records.

CP-6(1)	Separation from Primary Site (High, Moderate)	P1

Control:

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental 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 threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; and other relevant documents or records.

CP-6(2)	Recovery Time/Point Objectives (High)	P2

Control:

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Supplemental Guidance:

None.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate storage site; and other relevant documents or records.

CP-6(3)	Accessibility (High, Moderate)	P1

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.

Supplemental Guidance:

Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations 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.

Reference(s): FedRAMP Rev. 4 Baseline	Related Controls Requirement(s): RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; mitigation actions for accessibility problems to the alternate storage site; and other relevant documents or records.

CP-7	Alternate Processing Site (High, Moderate)	P1

Control:

The organization:
a. Establishes an alternate processing site, including necessary agreements to permit the transfer and resumption of information system operation types defined by CMS for essential missions/business functions within an allowable outage time as specified by the system contingency plan or COOP for the business function(s) supported by the system 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 that of the primary site.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization defines a resumption time period consistent with the recovery time objectives and business impact analysis. The resumption time period is approved and accepted by the Joint Authorization Board (JAB).

Supplemental Guidance:

Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability if 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 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 CMS-defined 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 CMS recovery time objectives.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When an alternate processing site is used, administrative, physical and technical controls must be implemented to protect personally identifiable information (PII) in accordance with the privacy risks identified.

Guidance for systems processing, storing, or transmitting PHI:

When an alternate processing site is used, administrative, physical and technical controls must be implemented to protect PHI in accordance with the organization's risk analysis.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(a)(2)(i), 45 C.F.R. §164.308(7)(ii)(C); NIST SP: 800-34; PPD-21;	**Related Controls Requirement(s):** CP-2, CP-6, CP-8, CP-9, CP-10, MA-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; system security plan; spare equipment and supplies at alternate processing site; equipment and supply contracts; service level agreements; and other relevant documents or records.

CP-7(1)	Separation from Primary Site (High, Moderate)	P1

Control:

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Supplemental 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 threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; and other relevant documents or records.

CP-7(2)	Accessibility (High, Moderate)	P1

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.

Supplemental Guidance:

Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; and other relevant documents or records.

CP-7(3)	Priority of Service (High, Moderate)	P1

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).

Supplemental Guidance:

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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; and other relevant documents or records.

CP-7(4)	Preparation for Use (High)	P2

Control:

The organization prepares the alternate processing site so the site is ready to be used as the operational site supporting essential CMS missions and business functions.

Supplemental Guidance:

Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place.

Reference(s):	**Related Controls Requirement(s):** CM-2, CM-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; and other relevant documents or records.
Test: Information system at the alternate processing site.

CP-8	Telecommunications Services (High, Moderate)	P1

Control:

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential CMS missions and business functions within the resumption time specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Implementation Standards:

High:

Std.1 - Ensure alternate telecommunications service level agreements (SLAs) are in place to permit resumption of system Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtimes (MTD).
Std.2 - Ensure alternate telecommunications service agreements are in place to permit resumption of information system operations for essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable.

Moderate:

Std.1 - Ensure alternate telecommunications service level agreements (SLAs) are in place to permit resumption of system Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtimes (MTD).

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization defines a resumption time period consistent with the recovery time objectives and business impact analysis. The resumption time period is approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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 alternate telecommunications agreements.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-3; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B); NIST SP: 800-34; Web: tsp.ncs.gov	**Related Controls Requirement(s):** CP-2, CP-6, CP-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; system security plan; primary and alternate telecommunications service agreements; list of essential missions and business functions; and other relevant documents or records.

CP-8(1)	Priority of Service Provisions (High, Moderate)	P1

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 if the primary and/or alternate telecommunications services are provided by a common carrier.

Supplemental Guidance:

Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; and other relevant documents or records.

CP-8(2)	Single Points of Failure (High, Moderate)	P1

Control:

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

CP-8(3)	Separation of Primary/Alternate Providers (High)	P2

Control:

The organization obtains alternate telecommunications services from providers that are separated from primary service providers so as not to be susceptible to the same hazards.

Supplemental Guidance:

Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; alternate telecommunications service provider's site; primary telecommunications service provider's site; and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

CP-8(4)	Provider Contingency Plan (High)	P2

Control:

The organization:
a. Requires primary and alternate telecommunications service providers to have contingency plans;
b. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and
c. Obtains evidence of contingency testing/training by providers within every 365 days.

Supplemental Guidance:

Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with DHS and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; and other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers.

CP-9	Information System Backup (High, Moderate, Low)	P1

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 and other forms of data, including paper records within the defined 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:

High & Moderate:

Std.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 plus 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.
Std.2 - Backups must be compliant with CMS requirements for protecting data at rest. (see SC-28)

Low:

Std.1 - Perform backups of user-level and system-level information (including system state information) every month.
Std.2 - Backups must be compliant with CMS requirements for protecting data at rest. (see SC-28)

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Ensure that a current, retrievable, copy of personally identifiable information (PII) is available before movement of servers.
PRIV.2 - Use the encryption methodology specified in SC-13 to encrypt personally identifiable information (PII) confidentiality impact level information in backups at the storage location.

Systems processing, storing, or transmitting PHI:

PHI.1 - Establish procedures that create a retrievable, exact copy of the PHI before any movement of information system equipment.

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement these Standards (CP-9 CSP.1 – CSP.6) as replacements for the above Control (CP-9) and Implementation Standards (High & Moderate Std.1 and Std.2; Low Std.1 and Std.2; PRIV.1 and PRIV.2; and PHI.1). The organization must determine what elements of the cloud environment require the Information System Backup control. The cloud environment elements requiring Information System Backup are approved and accepted by the Joint Authorization Board (JAB).
CSP.2 - For CSPs, the organization determines how Information System Backup is going to be verified and appropriate periodicity of the check. The verification and periodicity of the Information System Backup are approved and accepted by the JAB.
CSP.3 - For CSPs, the organization:
(a) Conducts backups of user-level information contained in the information system daily (incremental) and weekly (full);
(b) Conducts backups of system-level information contained in the information system daily (incremental) and weekly (full); and
(c) Conducts backups of information system documentation, including security-related documentation daily (incremental) and weekly (full).
CSP.4 - For CSPs, the organization maintains at least three (3) backup copies of user-level information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.
CSP.5 - For CSPs, the organization maintains at least three (3) backup copies of system-level information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.
CSP.6 - For CSPs, the organization maintains at least three (3) backup copies of information system documentation including security information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.

Low:

CSP.1 - CSPs must implement these Standards (CP-9 CSP.1 – CSP.6) as replacements for the above Control (CP-9) and Implementation Standards (High & Moderate Std.1 and Std.2; Low Std.1 and Std.2; PRIV.1 and PRIV.2; and PHI.1). The organization must determine what elements of the cloud environment require the Information System Backup control. The cloud environment elements requiring Information System Backup are approved and accepted by the JAB.
CSP.2 - For CSPs, the organization determines how Information System Backup is going to be verified and appropriate periodicity of the check. The verification and periodicity of the Information System Backup are approved and accepted by the JAB.
CSP.3 - For CSPs, the organization:
(a) Conducts backups of user-level information contained in the information system daily (incremental) and weekly (full);
(b) Conducts backups of system-level information contained in the information system daily (incremental) and weekly (full); and
(c) Conducts backups of information system documentation, including security-related documentation daily (incremental) and weekly (full).
CSP.4 - For CSPs, the organization maintains at least three (3) backup copies of user-level information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.
CSP.5 - For CSPs, the organization maintains at least three (3) backup copies of system-level information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.
CSP.6 - For CSPs, the organization maintains at least three (3) backup copies of information system documentation including security information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.

Supplemental Guidance:

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 CMS 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Backup copies of information need to be protected with the same level of security as if that information were being maintained on the original information system. Applicable controls necessary to achieve this and to protect confidentiality include encryption of the backup. Backing up information helps maintain the integrity of the data—a requirement of the Privacy Act and HIPAA.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(d)(2)(iv), 164.312(c)(1), 45 C.F.R. §164.308(a)(7)(ii)(C); NIST SP: 800-34	**Related Controls Requirement(s):** CP-2, CP-6, MP-4, MP-5, SC-13, SC-28

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; system security plan; backup storage location(s); information system backup logs or records; and other relevant documents or records.
Interview: Organizational personnel with information system backup responsibilities.

CP-9(1)	Testing for Reliability/Integrity (High, Moderate)	P1

Control:

The organization tests backup information following each backup, at least every three months for High systems or six months for Moderate systems, to verify media reliability and information integrity.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (CP-9(1) CSP.1) as a replacement for the above Control Enhancement (CP-9(1)). The organization tests backup information no less often than at least every 365 days.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** CP-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; system security plan; information system backup test results; backup storage location(s); and other relevant documents or records.

CP-9(2)	Test Restoration Using Sampling (High)	P2

Control:

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

Supplemental Guidance:

None.

Reference(s):	Related Controls Requirement(s): CP-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system backup test results; contingency plan testing and/or exercise documentation; contingency plan test results; and other relevant documents or records.

CP-9(3)	Separate Storage for Critical Information (High)	P1

Control:

The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

Systems defined as CSPs:

The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (CP-9(3) CSP.1) as a replacement for the above Control Enhancement (CP-9(3)). The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

Supplemental Guidance:

Critical system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations.

Guidance for systems defined as CSPs:

Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations.

Reference(s): FedRAMP Rev. 4 Baseline	Related Controls Requirement(s): CM-2, CM-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization stores backup copies of operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; backup storage location(s); and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information system backup responsibilities.

Systems defined as CSPs:

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; backup storage location(s); and other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information system backup responsibilities.

CP-9(5)	Transfer to Alternate Storage Site (High)	P2

Control:

The organization transfers information system backup information to the alternate storage site at defined time periods (defined in the applicable security plan) and transfer rates (defined in the applicable security plan) consistent with the recovery time and recovery point objectives.

Supplemental Guidance:

Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; system security plan; information system backup test results; alternate site service agreements; backup storage location(s); and other relevant documents or records.

CP-10	Information System Recovery and Reconstitution (High, Moderate, Low)	P1

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 must be done in a trusted, secure, and verifiable manner.

Implementation Standards:

High, Moderate, & Low:

Std.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.

Supplemental Guidance:

Recovery is executing information system contingency plan activities to restore CMS 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Information system recovery and reconstitution is an important step to restoring sensitive information, such as both personally identifiable information (PII) and protected health information (PHI), to an accurate state following execution of a contingency plan.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST SP: 800-34	**Related Controls Requirement(s):** CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; and other relevant documents or records.
Test: Automated mechanisms and/or manual procedures for implementing information system recovery and reconstitution operations.

CP-10(2)	Transaction Recovery (High, Moderate)	P1

Control:

The information system implements transaction recovery for systems that are transaction-based.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-34	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 results; and other relevant documents or records.
Test: Automated mechanisms implementing transaction recovery capability.

CP-10(4)	Restore within Time Period (High)	P1

Control:

The organization provides the capability to restore information system components within the target restoration time from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Supplemental Guidance:

Restoration of information system components includes, for example, reimaging which restores components to known, operational states.

Reference(s): NIST SP: 800-34	**Related Controls Requirement(s):** CM-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Interview: Organizational personnel with information system recovery and reconstitution responsibilities.

B.7 Identification and Authentication (IA)

IA-1	Identification and Authentication Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

b. Reviews and updates (as necessary) the current:

1. Identification and authentication policy at least every three (3) years; and

2. Identification and authentication procedures at least every three (3) years.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 201; FISCAM: AS-1, SM-1, SM-3; NIST SP: 800-12, 800-63, 800-73, 800-76, 800-78, 800-100	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy and procedures; other relevant documents or records.
Interview: Organizational personnel with identification and authentication responsibilities.

IA-2	Identification and Authentication (Organizational Users) (High, Moderate, Low)	P1

Control:

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Implementation Standards:

High, Moderate, & Low:

Std.1 - Require the use of system and/or network authenticators and unique user identifiers.
Std.2 - Help desk support requires user identification for any transaction that has information security implications.

Supplemental Guidance:

Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, 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 VPNs 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.

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., a biometric identifier). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government PIV card and the Department of Defense (DoD) common access card. 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Implementing this control ensures unique identification of an individual's account, preventing anonymous access to sensitive information such as personally identifiable information (PII) and providing appropriate access (e.g., where there is a need for the PII in the performance of the user's official duties) for organizational users. The HIPAA Security Rule requires that organizations uniquely identify users and implement procedures to verify user identity.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2, 201; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d); Homeland Security Presidential Directive (HSPD) -12; NIST SP: 800-63, 800-73, 800-76, 800-78; OMB Memo: M-04-04, M-06-16, M-11-11, M-16-04; Web: idmanagement.gov	**Related Controls Requirement(s):** AC-2, AC-3, AC-14, AC- 17, AC-18, IA-4, IA-5, IA-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Examine: Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Examples:
1. Privileged escalation mechanisms (tools) require authentication; and
2. Use of shared accounts, to include privileged accounts, is minimized or not used.
Examine: Information system enforces approved multifactor authentication for network access to systems processing or storing CMS sensitive information.
Test: Automated mechanisms implementing identification and authentication capability, to include strong authentication as required, for the information system.

IA-2(1)	Network Access to Privileged Accounts (High, Moderate, Low)	P1

Control:

The information system implements multifactor authentication (MFA) for network access to privileged accounts.

Supplemental Guidance:

Multifactor authentication requires the use of two or more different factors to achieve authentication. Factors are defined as follows: something you know, for example, a password or personal identification number (PIN); something you have, for example, a physical authenticator or cryptographic identification device; or something you are, for example, a biometric. Multifactor solutions that feature physical authenticators include, for example, hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD common access card. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, or remote) privileged accounts are always authenticated using multifactor options appropriate for the level of risk.
Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access. Authentication mechanisms must comply with the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	**Related Controls Requirement(s):** AC-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Examine: Information system enforces approved multifactor authentication for network access to privileged accounts.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(2)	Network Access to Non-Privileged Accounts (High, Moderate)	P1

Control:

The information system implements MFA for network access to non-privileged accounts.

Supplemental Guidance:

Multifactor authentication requires the use of two or more different factors to achieve authentication. Factors are defined as follows: something you know, for example, a personal identification number (PIN); something you have, for example, a physical authenticator or cryptographic private key stored in hardware or software; or something you are, for example, a biometric. Multifactor solutions that feature physical authenticators include, for example, hardware authenticators providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card or the DoD common access card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Organizations can also provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.
Authentication mechanisms must comply with the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 non-privileged information system accounts; and other relevant documents or records.
Examine: Information system enforces approved MFA for network access to non-privileged accounts.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(3)	Local Access to Privileged Accounts (High, Moderate)	P1

Control:

The information system implements MFA for local access to privileged accounts.

Supplemental Guidance:

Authentication mechanisms must comply with the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	**Related Controls Requirement(s):** AC-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Examine: Information system enforces approved MFA for local access to privileged accounts.
Test: Automated mechanisms implementing identification and authentication capability for the information system. System and application management accounts need to be checked.

IA-2(4)	Local Access to Non-Privileged Accounts (High)	P1

Control:

The information system implements MFA for local access to non-privileged accounts.

Supplemental Guidance:

Authentication mechanisms must comply with the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Reference(s): FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 non-privileged information system accounts; and other relevant documents or records.
Examine: Information system enforces approved MFA for local access to non-privileged accounts.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(6)	Non-Mandatory: Network Access to Privileged Accounts – Separate Device	P3

Control:

The information system implements MFA for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets minimum token requirements discussed in the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Supplemental Guidance:

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Requiring MFA to privileged accounts provides added assurance that a privileged user, who likely has elevated privileges with access to sensitive information such as PII, has proven their identity during the authentication process. OMB policy requires the use of two-factor authentication with one factor being separate from the computer itself. MFA provides heightened assurance of identity during the authentication process. OMB policy requires the use of two-factor authentication with one factor being separate from the computer itself. A separate device would include a Common Access Card (CAC). This control is required when the network access is remote (from outside the organization-controlled networks).

Reference(s): FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	**Related Controls Requirement(s):** AC-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Examine: Information system enforces approved multifactor authentication for network access to privileged accounts that is compliant with CMS Authentication Standards.
Test: Automated mechanisms supporting and/or implementing multifactor authentication capability. NOTE: System and application management accounts need to be checked.

IA-2(7)	Non-Mandatory: Network Access to Non-Privileged Accounts – Separate Device	P3

Control:

The information system implements MFA for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets minimum token requirements discussed in the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Supplemental Guidance:

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control is required for remote network access to information systems containing personally identifiable information (PII) (from outside the organization controlled networks). A separate device could include a common access card (CAC).

Reference(s): FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 non-privileged information system accounts; and other relevant documents or records.
Examine: Information system enforces approved MFA for network access to non-privileged accounts that is compliant with CMS Authentication Standards.
Test: Automated mechanisms supporting and/or implementing MFA capability.

IA-2(8)	Network Access to Privileged Accounts - Replay Resistant (High, Moderate)	P1

Control:

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (IA-2(8) CSP.1) as a replacement for the above Control Enhancement (IA-2(8)). The organization defines replay- resistant authentication mechanisms. The mechanisms are approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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 cryptographic nonces (e.g., an arbitrary number that may only be used once such as an RSA token numeric) or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(9)	Network Access to Non-Privileged Accounts - Replay Resistant (High)	P1

Control:

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Supplemental Guidance:

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

Reference(s): HIPAA: 164.312(a)(2)(i); OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(11)	Remote Access - Separate Device (High, Moderate, Low)	P1

Control:

The information system implements MFA for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets minimum token requirements discussed in the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Supplemental Guidance:

For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

A separate device could include a personal identity verification (PIV) card. This control is required when the network access is remote (from outside the organization controlled networks).

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	**Related Controls Requirement(s):** AC-6, SC-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 non-privileged information system accounts; and other relevant documents or records.
Examine: Information system enforces approved multifactor authentication that is compliant with CMS authentication standards.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(12)	Acceptance of PIV Credentials (High, Moderate, Low)	P1

Control:

The information system accepts and electronically verifies PIV credentials.

Supplemental Guidance:

This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). PIV credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AU-2, PE-3, SA-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Test: Automated mechanisms implementing PIV credential capability for the information system.

IA-3	Device Identification and Authentication (High, Moderate)	P1

Control:

The information system uniquely identifies and authenticates defined types of devices (defined in the applicable security plan) that require authentication mechanisms, which, at a minimum, use shared information (MAC or IP address) and access control lists to control remote network access prior to establishing the connection. If remote authentication is provided by the system itself, the system must follow OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (IA-3) CSP.1) as a replacement for the above Control (IA-3). The organization defines a list a specific devices and/or types of devices. The list of devices and/or device types is approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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 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, CMS information systems should be filtered by MAC and/or IP address when accessing remote systems.

Guidance for systems processing, storing, or transmitting PHI:

Implementing this control ensures that un-authenticated devices, e.g., mobile devices and personal laptop computers, are not able to make a connection to an information system containing PHI. HIPAA requires technical policies and procedures for systems that maintain PHI to allow access only to those persons or software programs that have been granted access rights.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(a)(1);	**Related Controls Requirement(s):** AC-17, AC-18, AC-19, CA-3, IA-4, IA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Test: Automated mechanisms implementing device identification and authentication.

IA-4	Identifier Management (High, Moderate, Low)	P1

Control:

The organization manages information system identifiers by:
a. Receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of three (3) years or more has passed; and
e. Disabling the identifier after the following periods of in activity: 30 days for High, 60 days for Moderate, or 90 days for Low systems.

Systems processing, storing, or transmitting PII (to include PHI):

Social security numbers (SSNs), and parts of SSNs, must not be used as system identifiers. Identifier management must ensure that any access to, or action involving, personally identifiable information (PII) is attributable to a unique individual.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, 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.
CSP.2 - For CSPs, the organization defines time period of inactivity for device identifiers. The time period is approved and accepted by the Joint Authorization Board (JAB).

Supplemental Guidance:

Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Identifiers are a critical and necessary function to confirm which people and devices are accessing sensitive information such as PII. Using SSNs as identifiers may create the potential for unauthorized disclosure of the SSN and linkage of that individual to other PII, as system identifiers are not protected with the same level of security as are database elements or passwords. In addition, collecting an individual's SSN may create notice requirements under the Privacy Act.

Guidance for systems processing, storing, or transmitting PHI:

Identifier management must ensure that any access to, or action involving, PHI is attributable to a unique individual.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d); 45 C.F.R. §164.308(a)(4); 45 C.F.R. §164.308(a)(5)(ii)(D)	**Related Controls Requirement(s):** AC-2, IA-2, IA-3, IA-5, IA- 8, SC-37

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system 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; and other relevant documents or records.
Interview: Organizational personnel with identifier management responsibilities.

IA-5	Authenticator Management (High, Moderate, Low)	P1

Control:

Non-standard account-authenticator management specifications are addressed in the CMS RMH, *Volume III, Standard 4.3, Non-Standard Authenticator Management*. For all others, 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:
- Passwords are valid for no longer than the period directed in IA-5(1) immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied passwords);
- PIV compliant access cards are valid for no longer than five (5) years;
- PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years; and
- Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked.
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.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization manages information system authenticators for users and devices by changing/refreshing authenticators every sixty (60) days by authenticator type.

Supplemental 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Adequate security to ensure confidentiality for an information system containing sensitive information such as personally identifiable information (PII) is achieved through the management of the authenticators permitting access to that system. Authenticator management includes periodically changing passwords or other identifiers (e.g., certification and signatures) to reinforce identity validation and adherence to administrative security policies as well as enforces a time-based restriction on access, all of which bound access to PII in some way, limiting exposure in the event a user account is compromised.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 201; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D); NIST SP: 800-63, 800-73, 800-76, 800-78; OMB Memo: M-04-04, M-11-11; Web: idmanagement.gov; 45 C.F.R. §164.308(a)(3); 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(d)	**Related Controls 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

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 accounts; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for determining initial authenticator content.
Test: Automated mechanisms implementing authenticator management functions.

IA-5(1)	Password-Based Authentication (High, Moderate, Low)	P1

Control:

Non-standard account-authenticator management specifications are addressed in the CMS RMH, *Volume III, Standard 4.3, Non-Standard Authenticator Management*. For all other password-based authentication, the information systems follow the direction in the applicable baseline configurations per CM-6, or if more stringent, the information system, for password-based authentication:
a. Prohibits the use of dictionary names or words;
b. Meets or exceeds enforcement of the following minimum password requirements:
- MinimumPasswordAge = one (1) day;
- MaximumPasswordAge = sixty (60) days;
- MinimumPasswordLength = Minimum length of eight (8) characters for regular user passwords, and minimum length of fifteen (15) characters for administrators or privileged user passwords;
- PasswordComplexity = minimum (three (3) for High or one (1) for Moderate or Low) character(s) from the four (4) character categories (A-Z, a-z, 0-9, special characters; and
- PasswordHistorySize = twelve (12) passwords for High or six (6) passwords for Moderate or Low systems.
c. The minimum length (MinimumPasswordLength) for administrators or privileged users is fifteen (15) characters;
d. If the operating environment enforces a minimum of number of changed characters when new passwords are created, set the value at twelve (12) for High and six (6) for Moderate or Low systems;
e. Stores and transmits only encrypted representations of passwords; and
f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - CSPs must implement this Standard (IA-5(1) CSP.1) as a replacement for the above Control Enhancement (IA-5(1)). The information system, for password- based authentication: (a) Enforces minimum password complexity of case sensitive, minimum of twelve (12) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters; (b) Enforces at least one (1) changed character or as determined by the information system (where possible) when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of one (1) day minimum, sixty (60) days maximum; and (e) Prohibits password reuse for twenty four (24) generations.
CSP.2 - Mobile devices are excluded from the password complexity requirement.

Supplemental 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., PIV cards). The implementation of such password mechanisms may not meet all the requirements in the control enhancement. Encrypted representations of 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.
Mobile devices are excluded from the password complexity requirement.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** IA-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Test: Automated mechanisms implementing authenticator management functions.

IA-5(2)	PKI-Based Authentication (High, Moderate)	P1

Control:

The information system, for PKI-based authentication:
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.

Supplemental Guidance:

Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor, including certificate policy processing.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** IA-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for PKI-based authentication management.
Test: Automated mechanisms implementing PKI-based authenticator management functions.

IA-5(3)	In-Person or Trusted Third-Party Registration (High, Moderate)	P1

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).

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization requires that the registration process for receiving HSPD-12 smart cards be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; and other relevant documents or records.
Interview: Organizational personnel with authenticator management responsibilities.

IA-5(11)	Hardware Token-Based Authentication (High, Moderate, Low)	P1

Control:

The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Supplemental Guidance:

Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government PIV card. Organizations define specific requirements for tokens, such as those associated with PKI.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.

IA-6	Authenticator Feedback (High, Moderate, Low)	P2

Control:

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental 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, for example, mobile devices with 2-4 inch screens, this threat may be less significant, 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.

Guidance for systems processing, storing, or transmitting PHI:

Restricting feedback from the authentication process limits ability of unauthorized users to compromise the authentication mechanisms for accounts that can access PHI. Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(a)(1)	**Related Controls Requirement(s):** PE-18

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; system security plan; information system design documentation; information system configuration settings and associated documentation; application code reviews for authentication mechanisms; and other relevant documents or records.
Interview: Organizational personnel with responsibility for authentication mechanisms.
Test: Authentication mechanisms on all interfaces. Verify that each authentication mechanism obscures authentication information during input and/or authentication attempt. Determine whether the method used to obscure authentication information is appropriate for the information type and display location (see Supplemental Guidance).

IA-7	Cryptographic Module Authentication (High, Moderate, Low)	P1

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.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Information systems containing personally identifiable information (PII) must use FIPS 140-2 validated cryptographic modules.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 140; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R.§164.312(a)(2)(iv) Web: csrc.nist.gov/groups/STM/cmvp/index.html;	**Related Controls Requirement(s):** SC-12, SC-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; system security plan; information system design documentation; information system configuration settings and associated documentation; application code reviews for cryptographic module implementation and/or use; FIPS 140-2 validation certificate number(s) for implemented cryptographic module(s); and other relevant documents or records.
Interview: Organizational personnel with responsibility for cryptographic mechanisms.
Test: Authentication mechanisms on all cryptographic modules. Verify that each cryptographic module has a FIPS 140-2 validation certificate and is operating in the FIPS- approved mode of operation. Verify that all authentication mechanisms for each cryptographic module meet the requirements of all control-specified requirements.

IA-8 | Identification and Authentication (Non-Organizational Users) (High, Moderate, Low) | P1

Control:

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users) prior to gaining access to all Department systems and networks (unless a risk-based decision is made for a system that does not require non-organization user authentication).

Supplemental 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.
If E-Authentication is used, refer to Risk Management Handbook (RMH), *Volume III, Standard 3.1, CMS Authentication Standards*.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Like IA-2, this control requires information systems to uniquely identify and authenticate system users that are not part of the organization as well as processes that act on behalf of another organization. This means no one is provided anonymous access to sensitive information, such as personally identifiable information (PII), and supports managing each user's appropriate access to sensitive information.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 201; NIST SP: 800-63, 800-116; OMB Memo: M-04-04, M-10-06-2011, M-11-11; Web: idmanagement.gov; 45 C.F.R. §164.312(a)(2)(i)	**Related Controls Requirement(s):** AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-8(1)	Acceptance of PIV Credentials from Other Agencies (High, Moderate, Low)	P1

Control:

The information system accepts and electronically verifies PIV credentials from other federal agencies.

Supplemental Guidance:

This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 201	**Related Controls Requirement(s):** AU-2, PE-3, SA-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; PIV credential documentation; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for PIV credential management.

IA-8(2)	Acceptance of Third-Party Credentials (High, Moderate, Low)	P1

Control:

The information system accepts only FICAM-approved third-party credentials.

Supplemental Guidance:

This control enhancement typically applies to organizational information systems that are accessible to the public, for example, public-facing websites. Third-party credentials are those credentials issued by non-federal government entities approved by the Federal Identity, Credential and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows Federal Government relying parties to trust such credentials at their approved assurance levels.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 201	**Related Controls Requirement(s):** AU-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; FICAM credential documentation; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for FICAM credential management.

IA-8(3)	Use of FICAM-Approved Products (High, Moderate, Low)	P1

Control:

The organization employs only FICAM-approved information system components in information systems that authenticate non-organizational users and accept third-party credentials.

Supplemental Guidance:

This control enhancement typically applies to information systems that are accessible to the public, for example, public-facing websites.

FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the FICAM Conformance Program.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 201	**Related Controls Requirement(s):** SA-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; FICAM-approved information system component procedures; and other relevant documents or records. **Interview:** Organizational personnel with responsibilities for FICAM-approved information system component management.

IA-8(4)	Use of FICAM-Issued Profiles (High, Moderate, Low)	P1

Control:

The information system conforms to FICAM-issued profiles.

Supplemental Guidance:

This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange).

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 201	**Related Controls Requirement(s):** SA-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; FICAM-issued credential documentation; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for FICAM-issued credential management.

B.8 Incident Response (IR)

IR-1	Incident Response Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls.

b. Reviews and updates (as necessary) the current:

1. Incident response policy within every three (3) years; and
2. Incident response procedures within every three (3) years.

Systems processing, storing, or transmitting PII (to include PHI):

Applicable personnel (item a) include the Incident Response Team as required by OMB M-17-12.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

In developing incident response policy and procedures, ensure those policies and procedures incorporates guidance from the privacy office for the handling of incidents involving personally identifiable information (PII).

Guidance for systems processing, storing, or transmitting PHI:

In developing incident response policy and procedures, ensure those policies and procedures incorporates guidance from the privacy office for the handling of incidents involving PHI.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-1, AS-2, SM-1, SM-3; HIPAA: 45 C.F.R.§164.308(a)(6)(i); 45 C.F.R. §164.530(b)(1); NIST SP: 800-12, 800-61, 800-83, 800-100	**Related Controls Requirement(s):** PM-9, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response; system security plan; incident response plan; and other relevant documents or records.
Interview: Organizational personnel with incident response operational responsibilities.

IR-2	Incident Response Training (High, Moderate, Low)	Assurance	P2

Control:

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
a. Within one (1) month of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Formally tracks personnel participating in incident response training.

Supplemental Guidance:

Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who 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. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Those responsible for identifying and responding to a security incident must understand how to recognize when sensitive information such as personally identifiable information (PII) or protected health information (PHI) is involved so that they can coordinate with the designated (e.g., privacy) official.

Reference(s): FedRAMP Rev. 4 Baseline; Federal Information Systems Controls Audit Manual (FISCAM): AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(6)(i); NIST SP: 800-16, 800-50; OMB Memo: M-16-04	**Related Controls Requirement(s):** AT-3, CP-3, IR-8, AR-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization identifies personnel with incident response roles and responsibilities with respect to the information system;
(ii) The organization provides incident response training to information system users consistent with assigned roles and responsibilities;
(iii) Incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;
(iv) The organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training in accordance with an organization-defined frequency;
(v) The organization provides refresher incident response training in accordance with an organization-defined frequency; and
(vi) The organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response training; incident response training materials; system security plan; incident response plan; incident response training records; and other relevant documents or records.
Examine: Information system includes capability to track participation in incident response training activities.
Interview: Organizational personnel with incident response training and operational responsibilities

IR-2(1)	Simulated Events (High)	Assurance	P2

Control:

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Supplemental Guidance:

None.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response training and incident response.
Interview: Organizational personnel with incident response training and operational responsibilities.

IR-2(2)	Automated Training Environments (High)	Assurance	P2

Control:

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

Supplemental Guidance:

None.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response training; incident response training material; system security plan; incident response plan; incident response training records; and other relevant documents or records.
Examine: Information system implements automated mechanisms to provide a thorough and realistic incident response training environment.
Interview: Organizational personnel with incident response training and operational responsibilities.

IR-3	Incident Response Testing (High, Moderate)	Assurance	P2

Control:

The organization tests the incident response capability for the information system within every three hundred sixty-five (365) days using NIST SP 800-61, reviews, analyses, and simulations to determine the organization's incident response effectiveness, and documents its findings.

Implementation Standards:

High & Moderate:

Std.1 - Incident response capability tests must exercise (or simulate exercise of) all organizational response capabilities. The organization's documented response to an actual historic incident may be used as part of an incident response capability test, and any response capabilities that were not exercised as part of the previous actual incident response activities must be additionally exercised (or simulated) as part of the test.

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization defines tests and/or exercises in accordance with NIST SP 800-61 (as amended).
CSP.2 - For CSPs, the organization provides test plans to FedRAMP at least every 365 days. Test plans are approved and accepted by the Joint Authorization Board (JAB) prior to commencing testing.

Supplemental Guidance:

Organizations test incident response capabilities to determine the overall effectiveness of its 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 the incident response activities themselves. In other words: an institution's resources may be consumed and depleted both directly by an incident, and by its need to allocate resources to address the incident. If the organization routinely responds to incidents, and follows the documented incident response plan to do so, then full-scale simulations (or "table-top exercises") might not be necessary, especially if the documentation produced from the incident response is sufficient to provide a thorough understanding of the breadth and depth of the organization's analysis and response to the incident (including lessons learned). However, it is often the case that responses to incidents do not exercise the full incident response plan (for example, an incident might not meet the documented threshold requiring the organization to alert the media about the incident). If the organization uses a historic response to an incident as the basis for the annual incident response capability test, any parts of the incident response capability that were not exercised in the historic response must be tested (either via actual exercises or through simulation) and documented as part of the capability test.

Guidance for systems defined as CSPs:

If the organization routinely responds to incidents, and follows the documented incident response plan to do so, then full-scale simulations (or "table-top exercises") might not be necessary, especially if the documentation produced from the incident response is sufficient to provide a thorough understanding of the breadth and depth of the organization's analysis and response to the incident (including lessons learned). However, it is often the case that responses to incidents do not exercise the full incident response plan (for example, an incident might not meet the documented threshold requiring the organization to alert the media about the incident). If the organization uses a historic response to an incident as the basis for the annual incident response capability test, any parts of the incident response capability that were not exercised in the historic response must be tested (either via actual exercises or through simulation) and documented as part of the capability test.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(6)(i); NIST SP: 800-84, 800-115; OMB Memo: M-16-04	**Related Controls Requirement(s):** CP-4, IR-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization defines incident response tests;
(ii) The organization defines in the security plan, explicitly or by reference, the frequency of incident response tests and the frequency is at least every 365 days;
(iii) The organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization- defined frequency;
(iv) The organization documents the results of incident response tests/exercises; and
(v) The organization determines the effectiveness of the incident response capability.

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response testing; incident response test records; system security plan; incident response plan; and other relevant documents or records.
Examine: Records verify that the organization tests the incident response capability at least as often as required by control.
Examine: Records verify that the organization uses NIST SP 800-61-compliant reviews, analyses, and simulations to perform incident response capability tests.
Interview: Organizational personnel with responsibility for incident response.

IR-3(2)	Coordination with Related Plans (High, Moderate)	Assurance	P2

Control:

The organization coordinates incident response testing with organizational elements responsible for related plans.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization coordinates incident response testing with organizational elements responsible for related plans.

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response testing; incident response test records; system security plan; incident response plan; and other relevant documents or records.
Examine: Records verify that the organization coordinates tests of the incident response capability with other related organizational entities.
Interview: Organizational personnel with responsibility for incident response.

IR-4	Incident Handling (High, Moderate, Low)	P1

Control:

The organization:
a. Implements an incident handling capability (i.e., system incident response plan) using the current RMH, *Chapter 08: Incident Response*;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises and implements the resulting changes accordingly.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Document relevant information related to a security incident per the current CMS Incident Handling and Breach Notification Standard and Procedures.
Std.2 - Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow a chain of custody for forensic evidence.
Std.3 - Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure, including isolating or disconnecting systems.
Std.4 - Incident response activities, to include forensic malware analysis, is coordinated with the ISSO and the CCIC. Each organization's security operations center:
(a) Is responsible for actions to reduce the risk that an information security and/or privacy incident will occur and to respond appropriately to each incident or breach; and
(b) Maintains primary responsibility for incident detection, including internal security monitoring and analysis of network traffic and logs.
Std.5 - Contact information for individuals with incident handling responsibilities must be maintained in the system Incident Response Plan.
(a) Changes must be documented in the system Incident Response Plan within three (3) days of the change.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

Supplemental Guidance:

Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as 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 includes 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).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

A strategic, well-thought-out security incident response program will integrate with privacy incident and breach response where appropriate, with the two processes being mutually supportive.

Reference(s): Executive Order: 13587; FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HHS: Policy for Monitoring Employee Use of HHS IT Resources; HIPAA: 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. Part 164 Subpart D; NIST SP: 800-61; OMB Memo: M-16-04	**Related Controls Requirement(s):** AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization implements an incident handling capability for security incidents that includes:
- Preparation;
- Detection and analysis;
- Containment;
- Eradication; and
- Recovery.

(ii) The organization coordinates incident handling activities with contingency planning activities;
(iii) The organization incorporates lessons learned from ongoing incident handling activities into:
- Incident response procedures;
- Training; and
- Testing/exercises.

(iv) The organization implements the resulting changes to incident response procedures, training and testing/exercises accordingly; and
(v) The organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident handling; incident response plan; and other relevant documents or records.
Examine: System Incident Response Plan to ensure incident handling contact information is being maintained.
Interview: Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities.
Test: Incident handling capability for the organization.

IR-4(1)	Automated Incident Handling Processes (High, Moderate)	P1

Control:

The organization employs automated mechanisms to support the incident handling process.

Implementation Standards:

High:

Std.1 - Automated mechanisms support the exchange of incident handling information with the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal requirements;
(b) Incident handling information sources include systems, appliances, devices, services, and applications (including databases);
(c) Incident handling information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and
(d) CCIC directed incident handling information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.

Moderate:

Std.1 - Automated mechanisms support the exchange of incident handling information with the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal requirements;
(b) Incident handling information sources include systems, appliances, devices, services, and applications (including databases).
(c) Incident handling information sources that do not support the exchange of information with the CCIC must be documented in the applicable risk assessment and security plan; and
(d) CCIC directed incident handling information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw audit records must be available in an unaltered format to the CCIC.

Supplemental Guidance:

Automated mechanisms supporting incident handling processes include, for example, online incident management systems.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization:
(i) Employs automated mechanisms to support the incident handling process; and
(ii) Meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; and other relevant documents or records.
Examine: Information system provides an automated support for incident handling.
Interview: Organizational personnel with incident handling responsibilities.
Test: Automated mechanisms that support and/or implement the incident handling process.

IR-4(4)	Information Correlation (High)	P1

Control:

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Supplemental Guidance:

Sometimes the nature of a threat event, for example, a hostile cyber-attack, is such that it can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

Reference(s): NIST SP: 800-61r2; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization employs automated mechanisms to support the incident handling process.

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; and other relevant documents or records.
Examine: Information system provides automated support for incident information correlation.

Examine: Records demonstrating that the organization collects and correlates incident data from separate information systems to provide an organization-wide view of incident awareness and response.
Interview: Organizational personnel with incident handling responsibilities.

IR-4(6)	Non-Mandatory: Insider Threats – Specific Capabilities	P3

Control:

The organization defines and implements the incident handling capability for insider threats.

Supplemental Guidance:

While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses.

Reference(s): IS2P2; HHS: Policy for Monitoring Employee Use of HHS IT Resources	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization:
(i) Implements incident handling capability for insider threats; and
(ii) Meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident handling; incident response plan; and other relevant documents or records.
Interview: Organizational personnel with incident handling responsibilities.
Test: Insider threat incident handling capability for the organization.

IR-5	Incident Monitoring (High, Moderate, Low)	Assurance	P1

Control:

The organization tracks and documents all physical, information security, and privacy incidents.

Implementation Standards:

High, Moderate, & Low:

Std.1 - The organization forwards information system security and privacy incident and breach information:
- In accordance with reporting requirements defined under the current RMH, *Chapter 08: Incident Response* or applicable incident response plans, whichever is sooner; and
- Provides incident and breach information in format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements.

Supplemental 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.
Tracking and documenting security and privacy incidents enables the organization to respond more effectively and evaluate both individual incidents and trends across incidents over time.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Tracking and documenting security and privacy incidents enables the organization to respond more effectively and evaluate both individual incidents and trends across incidents over time.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. Part 164 Subpart D; NIST SP: 800-61, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization:
(i) Tracks and documents all physical, information system security, and privacy incidents;
(ii) Meets all the requirements specified in the applicable Implementation Standard(s); and
(iii) Has an organization-wide Security Information and Event Management (SIEM) capability. Additionally, SIEM information must be forwarded to the CCIC in accordance with CMS requirements.

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; and other relevant documents or records.
Examine: Information systems forward security and privacy event logs to a centralized management service for aggregation, analysis, and monitoring.
Interview: Organizational personnel with incident monitoring responsibilities.
Test: Incident monitoring capability for the organization.

IR-5(1)	Automated Tracking/Data Collection/Analysis (High)	Assurance	P1

Control:

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Supplemental Guidance:

Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers or other electronic databases of incidents.

Reference(s): NIST SP: 800-137	**Related Controls Requirement(s):** AU-7, IR-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident tracking and analysis; automated mechanisms supporting incident tracking and analysis; and other relevant documents or records.
Examine: Information system provides automated support for incident tracking and analysis.
Interview: Organizational personnel with incident handling responsibilities.
Test: Automated mechanisms that support and/or implement the incident tracking and analysis.

IR-6	Incident Reporting (High, Moderate, Low)	P1

Control:

The organization:
a. Requires personnel to report actual or suspected security and privacy incidents to the organizational incident response capability within the timeframe established in the current RMH, *Chapter 08: Incident Response*; and
b. Reports security incident information to authorities (defined in the applicable system security plan [SSP]) and in Implementation Standard 1.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Designated authorities must include the CCIC. The CCIC provides oversight of information security and privacy, to include incident reporting, for each FISMA system operated by or on behalf of CMS.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - CSPs must implement this Standard (IA-6 CSP.1) as a replacement for the above Control (IA-6). The organization requires personnel to report suspected security incidents to the organizational incident response capability within the United States Computer Emergency Readiness Team (US-CERT) incident reporting timelines as specified in NIST SP 800-61 (as amended).

Supplemental Guidance:

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. 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 federal laws, Executive Orders,

directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to US-CERT within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.
For more information see the see the RMH, *Chapter 08: Incident Response*.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Incidents involving personally identifiable information (PII) must be reported to the appropriate incident response center, e.g., US-CERT or Intelligence Community Security Coordination Center.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(6)(ii), 45 C.F.R. §164.314(a)(2)(i); 45 C.F.R. §164.314(a)(2)(i)(C); 45 C.F.R. Part 164 Subpart D; NIST SP: 800-61; OMB Memo: M-17-12, M-16-04; Web: us-cert.gov	**Related Controls Requirement(s):** IR-4, IR-5, IR-8, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current RMH, *Chapter 08: Incident Response*;
(ii) The organization reports security incident information to designated authorities; and
(iii) The organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; system security plan; incident response plan; and other relevant documents or records.
Examine: Information systems provide the functionality to report actual or suspected security incidents to the organizational incident response capability.
Examine: Organization facilitates required oversight of incident reporting by CMS (including coordination and cooperation with the CCIC).
Interview: Organizational personnel with incident reporting responsibilities.
Test: Organizational processes for incident reporting; automated mechanisms supporting and/or implementing reporting of incident information.

IR-6(1)	Automated Reporting (High, Moderate)	P1

Control:

The organization employs automated mechanisms to assist in the reporting of security incidents.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-61; Web: us-cert.gov	**Related Controls Requirement(s):** IR-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; and other relevant documents or records.
Examine: Information system provides automated support for incident reporting.
Interview: Organizational personnel with incident handling responsibilities.
Test: Automated mechanisms that support and/or implement incident reporting.

IR-7	Incident Response Assistance (High, Moderate, Low)	P3

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.

Implementation Standards:

High, Moderate, & Low:

Std.1 - The CCIC provides centralized coordination and assistance on information security and privacy incident/breach awareness and management for all information systems across the CMS enterprise.

Supplemental Guidance:

Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. The CMS CISO is available for assistance at mailto:CISO@cms.hhs.gov.
Security incident response resources and privacy incident and breach response resources must know which resources are available, and how and when to coordinate.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Incident response assistance for incidents involving PII may include use of the forensic, technical, policy, and legal expertise of the organization's Information Assurance Officers/Managers, Privacy Officers, Legal Counsel, external or internal IT help desks, and the organization's Computer Emergency Response Team (CERT), in investigating and remediating incidents.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(6)(ii); OMB Memo: M-16-04; 45 C.F.R. §164.308(a)(6)(i)	**Related Controls Requirement(s):** AT-2, IR-4, IR-6, IR-8, SA-9, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents;
(ii) The incident response support resource is an integral part of the organization's incident response capability; and
(iii) The organization meets all the requirements specified in the applicable Implementation Standard(s).

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.
Interview: Organizational personnel with incident management responsibilities.

IR-7(1)	Automation Support for Availability of Information/Support (High, Moderate)	P2

Control:

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Supplemental 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 an incident response database capability to query interactively when seeking assistance or, conversely, the assistance capability may proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response-related information and support; automated mechanisms supporting incident response-related information and support and other relevant documents or records.
Examine: Information system provides automated support for pushing or pulling incident response-related information on demand by authorized users.
Interview: Organizational personnel with incident handling responsibilities.
Test: Automated mechanisms that support and/or implement incident response-related information push/pull.

IR-8	Incident Response Plan (High, Moderate, Low)	P1

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; and
8. Is reviewed and approved by the applicable Incident Response Team Leader;
b. Distributes copies of the incident response plan to:
- CMS Chief Information Security Officer;
- CMS Chief Information Officer;
- Information System Security Officer;
- CMS Office of the Inspector General/Computer Crimes Unit;
- All personnel within the organization Incident Response Team;
- All personnel within the PII Breach Response Team; and
- All personnel within the organization Operations Centers.
c. Reviews the incident response plan within every three hundred sixty-five (365) days;
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes to the organizational elements listed in b. above; and
f. Protects the incident response plan from unauthorized disclosure and modification.

Supplemental 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, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

In developing an incident response plan, ensure it incorporates guidance from the Privacy Office for the handling of incidents involving personally identifiable information (PII).

Guidance for systems processing, storing, or transmitting PHI:

In developing an incident response plan, ensure it incorporates guidance from the privacy office for the handling of incidents involving PHI.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-61; 45 C.F.R. §164.308(a)(6) C.F.R.	**Related Controls Requirement(s):** MP-2, MP-4, MP-5, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization develops an incident response plan that:
(i) Provides the organization with a roadmap for implementing its incident response capability;
(ii) Describes the structure and organization of the incident response capability;
(iii) Provides a high-level approach for how the incident response capability fits into the overall organization;
(iv) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
(v) Defines reportable incidents;
(vi) Provides metrics for measuring the incident response capability within the organization;
(vii) Defines the resources and management support needed to effectively maintain and mature an incident response capability;
(viii) Is reviewed and approved by the applicable Incident Response Team Leader; and
(ix) Is routinely followed in response to incidents.

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; and other relevant documents or records.
Interview: Organizational personnel with incident response planning responsibilities.
Test: Organizational incident response plan and related organizational processes.
NOTE: The organization incident response capability must be able to demonstrate knowledge of the incident response processes and procedures and evidence showing the plan is followed routinely while responding to incidents.

IR-10	Non-Mandatory: Integrated Information Security Analysis Team	P3

Control:

The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

Supplemental Guidance:

Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat to implement defensive measures that will enable organizations to deter intrusions more effectively. Moreover, it promotes the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated security analysis team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing intelligence development. This enables the team to identify adversary TTPs that are linked to the operations tempo or to specific missions/business functions, and to define responsive actions in a way that does not disrupt the mission/business operations. Ideally, information security analysis teams are distributed within organizations to make the capability more resilient.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The integrated information security analysis team will support the organization's personally identifiable information (PII) incident response team (as specified in OMB M-17-12) in all aspects of response to a security incident involving PII.

Reference(s): Cybersecurity Enhancement Act of 2014; OMB Memo: M-17-12, M-16-04	**Related Controls Requirement(s):** SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization:
(i) Establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel; and
(ii) Meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: Incident response policy; procedures addressing incident response planning and security analysis team integration; incident response plan; and other relevant documents or records.
Examine: Organization facilitates required oversight and coordination of information security and privacy incident response teams (including coordination and cooperation with the CCIC).
Interview: Organizational personnel with incident response and information security analysis responsibilities; organizational personnel with information security responsibilities; organizational personnel participating on integrated security analysis teams.

B.9 Maintenance (MA)

MA-1	System Maintenance Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.

b. Reviews and updates (as necessary) the current:

1. System maintenance policy within every three (3) years; and
2. System maintenance procedures within every three (3) years.

Systems processing, storing, or transmitting PII (to include PHI):

System maintenance policy and procedures must ensure that contractors having access to records (i.e., files or data) maintained in a system of records are contractually bound to be covered by the Privacy Act.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Privacy considerations should be included in system maintenance policy and procedures especially when the system contains information subject to the Privacy Act and/or HIPAA.

Guidance for systems processing, storing, or transmitting PHI:

Procedures to facilitate the implementation of the system maintenance policy should include access control validation and accountability procedures.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(d)(2)(iii); NIST SP: 800-12, 800-100	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities; system/network administrators.

MA-2	Controlled Maintenance (High, Moderate, Low)	P2

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 approves the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.

Supplemental 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, 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) 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.

Guidance for systems processing, storing, or transmitting PHI:

HIPAA requires organizations to apply reasonable and appropriate safeguards for the protection of PHI, including implementing policies and procedures to document repairs and modifications to the facility which are related to security.
Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(d)(2)(iii)	**Related Controls Requirement(s):** CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities; system/network administrators.
Test: Automated mechanisms supporting and/or implementing controlled maintenance; automated mechanisms implementing sanitization of information system components.

MA-2(2)	Automated Maintenance Activities (High)	P2

Control:

The organization:
a. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
b. Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

Supplemental Guidance:

None.

Reference(s):	Related Controls Requirement(s): CA-7, MA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities; system/network administrators.
Test: Automated mechanisms supporting and/or implementing controlled maintenance; automated mechanisms implementing sanitization of information system components.

MA-3	Maintenance Tools (High, Moderate)	P3

Control:

The organization approves, controls, and monitors information system maintenance tools.

Supplemental Guidance:

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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; NIST SP: 800-88	Related Controls Requirement(s): MA-2, MA-5, MP-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; and other relevant documents or records.

MA-3(1)	Inspect Tools (High, Moderate)	P3

Control:

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-88	**Related Controls Requirement(s):** SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; and other relevant documents or records.

MA-3(2)	Inspect Media (High, Moderate)	P3

Control:

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-88	**Related Controls Requirement(s):** SI-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; and other relevant documents or records.

MA-3(3)	Prevent Unauthorized Removal (High)	P3

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;
b. Sanitizing or destroying the equipment;
c. Retaining the equipment within the facility; or
d. Obtaining an exemption, in writing, from the CMS CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (MA-3(3) CSP.1) as a replacement for the above Control Enhancement (MA-3(3)). The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no sensitive information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.

Supplemental Guidance:

Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-88	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; and other relevant documents or records.

MA-4	Nonlocal Maintenance (High, Moderate, Low)	P2

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 strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions;
c. Maintains records for nonlocal maintenance and diagnostic activities; and
d. Terminates all sessions and network connections when nonlocal maintenance is completed.

Implementation Standards:

High, Moderate, & Low:

Std.1 - If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.
Std.2 - Media used during remote maintenance must be sanitized in accordance with NIST SP 800-88, as amended.

Supplemental 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 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.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2, 197, 201; FISCAM: AS-1, SM-7; NIST SP: 800-63, 800-88; 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(ii)	**Related Controls Requirement(s):** AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing nonlocal maintenance for the information system; system security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities

MA-4(1)	Auditing and Review (High, Moderate)	P2

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.

Supplemental Guidance:

None.

Reference(s):	**Related Controls Requirement(s):** AU-2, AU-6, AU-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing nonlocal maintenance for the information system; system security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities
Examine: Audit records for nonlocal maintenance and diagnostic sessions.
Examine: Documentation verifying that the organization performs reviews of audit records for nonlocal maintenance and diagnostic sessions.

MA-4(2)	Document Nonlocal Maintenance (High, Moderate)	P2

Control:

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing nonlocal maintenance for the information system; system security plan (SSP); information system design documentation; information system configuration settings and associated documentation; maintenance records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities
Examine: Documentation in the SSP of the policies and procedures covering maintenance and diagnostic connections.

MA-4(3)	Comparable Security/Sanitization (High)	P2

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 being serviced; or
b. Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (about organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (regarding potentially malicious software) before reconnecting the component to the information system.

Supplemental 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 being serviced.

Reference(s): NIST SP: 800-63, 800-88	**Related Controls Requirement(s):** MA-3, SA-12, SI-3, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing nonlocal maintenance for the information system; system security plan (SSP); information system design documentation; information system configuration settings and associated documentation; maintenance records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities
Examine: Documentation in the SSP of the policies and procedures covering maintenance and diagnostic connections.

MA-5	Maintenance Personnel (High, Moderate, Low)	P2

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.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

If maintenance personnel are contractors, then the organizations personnel responsible for contracting (such as the contracting officer [KO or CO], contracting officer's representative [COR], or contracting officer's technical representative [COTR]) or the program manager must ensure that contractors having access to records (i.e., files or data) from a system of records are contractually bound to be covered by the Privacy Act.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.310(d)(2)(iii)	**Related Controls Requirement(s):** AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3, SA-4, AR-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing maintenance personnel authorization; maintenance personnel rules of behavior; system security plan; maintenance records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities
Examine: Procedures governing maintenance personnel authorization, escort/supervision, and work execution.
Examine: Documentation verifying that the organization follows documented maintenance personnel policy and procedures.

MA-5(1) Individuals Without Appropriate Access (High) P2

Control:

The organization:
a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured.
b. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

Supplemental Guidance:

This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** MP-6, PL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing maintenance personnel that lack appropriate security clearances or citizenship; maintenance personnel rules of behavior; system security plan; maintenance records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities
Examine: Procedures governing maintenance personnel authorization, escort/supervision, and work execution.
Examine: Documentation verifying that the organization follows documented maintenance personnel policy and procedures, including sanitization of volatile storage components and removal of non-volatile storage components before non-cleared or non-US-citizen maintenance personnel initiate maintenance or diagnostic activities.

MA-6	Timely Maintenance (High, Moderate)	P2

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 RTO specified in the contingency plan.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs must implement this Standard (MA-6 CSP.1) as a replacement for the above Control (MA-6). The organization defines a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the Joint Authorization Board (JAB).
CSP.2 - For CSPs, the organization defines a time period to obtain maintenance and spare parts in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the JAB.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.310(a)(2)(iv)	**Related Controls Requirement(s):** 8, CP-2, CP-7, SA-14, SA-15

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system maintenance policy; procedures addressing maintenance for the information system; information system contingency plan; system security plan; vendor maintenance agreements; maintenance records; and other relevant documents or records.
Interview: Organizational personnel with information system maintenance responsibilities; system/network administrators.
Examine: Documentation verifying that maintenance support and/or spare parts are obtained within the applicable RTO specified in the contingency plan.

B.10 Media Protection (MP)

MP-1	Media Protection Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:
1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls.

b. Reviews and updates (as necessary) the current:
1. Media protection policy within every three (3) years; and
2. Media protection procedures within every three (3) years.

Systems processing, storing, or transmitting PII (to include PHI):

"Applicable personnel," as referred to in MP-1(a), includes employees and contractors with potential access to personally identifiable information (PII).

Systems processing, storing, or transmitting PHI:

"Applicable personnel," as referred to in MP-1(a), includes employees and contractors with potential access to protected health information (PHI).

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s):	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; and other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.

MP-2	Media Access (High, Moderate, Low)	P1

Control:

The organization restricts access to sensitive digital and non-digital media pursuant to Appendix I of the HHS Information *System Security and Privacy Policy* (IS2P) and in compliance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, to defined personnel or roles (defined in the applicable security plan) by disabling:
- disabling CD/DVD writers and allowing access to using CD/DVD viewing and downloading capabilities only to persons specified or in defined roles; and
- disabling USB ports and allowing access to using USB device capabilities only to persons specified or in defined roles.

Systems processing, storing, or transmitting PII (to include PHI):

Sensitive digital and non-digital media includes media containing personally identifiable information (PII). Defined personnel or roles must be authorized individuals with a valid need to know.

Systems processing, storing, or transmitting PHI:

Sensitive digital and non-digital media includes media containing protected health information (PHI).

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - CSPs must implement this Standard (MP-2 CSP.1) as a replacement for the above Control (MP-2). The organization defines types of digital and non-digital media. The media types are approved and accepted by the Joint Authorization Board (JAB).
CSP.2 - CSPs define a list of individuals with authorized access to defined media types. The list of authorized individuals is approved and accepted by the JAB.
CSP.3 - CSPs define the types of security measures to be used in protecting defined media types. The security measures are approved and accepted by the JAB.

Supplemental 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. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Restricting access to digital and non-digital media, including mobile devices with storage capabilities, protects sensitive information, such as PII, from unauthorized use and disclosure. A risk assessment should be conducted to determine what sensitive information if any, can be stored on certain media types and who is authorized to do so.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 164.312(c)(1); 45 C.F.R. §164.310(c); 45 C.F.R. §164.310(d)(1); NIST SP: 800-88, 800-111	**Related Controls Requirement(s):** AC-2, AC-3, IA-2, MP-4, PE-2, PE-3, PL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; and other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.

MP-3	Media Marking (High, Moderate)	P2

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 CMS CIO or his/her designated representative, from marking if the media remains within a secure environment.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs do not exempt any removable media types from marking.

Supplemental Guidance:

The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes regarding internal data structures within information systems (see AC-16). 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. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable.
However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Media containing personally identifiable information (PII), or the container for the media if labeling the media is not practicable, must be marked appropriately.

Guidance for systems processing, storing, or transmitting PHI:

Media containing PHI, or the container for the media if labeling the media is not practicable, must be marked appropriately.

Reference(s):	**Related Controls Requirement(s):** AC-16, PL-2, RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; system security plan; removable storage media and information system output; and other relevant documents or records.
Interview: Organizational personnel with information system media protection and marking responsibilities.

MP-4	Media Storage (High, Moderate)	P1

Control:

The organization:
a. Physically controls and securely stores digital and non-digital media defined within the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, and HHS IS2P Appendix I, within controlled areas; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Systems processing, storing, or transmitting PII (to include PHI):

Digital and non-digital media includes removable media that contains personally identifiable information (PII). This media must be stored a securable area or in a locked container.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - If PII is recorded on magnetic media with other data, the media should be protected as if all the data contained consisted of personally identifiable information.

Systems defined as CSPs:

High & Moderate:

CSP.1 - This Standard (MP-4 CSP.1) replaces MP-04 for Cloud Service Providers. The organization physically controls and securely stores magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks within organization-defined controlled areas; and, for digital media, the media are encrypted using a FIPS 140-2 validated module; and for non-digital media, the media are stored securely in locked cabinets or safes.
CSP.2 - CSPs define controlled areas within facilities where the information and information system reside.

Supplemental 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. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to a media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas or spaces for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.
Contact your CRA or the CCIC for the list of compliant formats.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Controlling the storage of media containing sensitive information such as PII protects the media from theft and promotes accountability.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.310(c), 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(iv); NIST SP: 800-56, 800-57, 800-88, 800-111	**Related Controls Requirement(s):** CP-6, CP-9, MP-2, MP-7, PE-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; system security plan; information system media; and other relevant documents or records.
Interview: Organizational personnel with information system media protection and storage responsibilities

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Cryptographic software licenses used to protect PII at rest.
Examine: PII magnetic media storage procedures.
Interview: Organizational personnel with PII protection responsibilities.

MP-5	Media Transport (High, Moderate)	P1

Control:

Commensurate with the FIPS 199 security categorizations for confidentiality and integrity of the data, the organization:
a. Protects and controls digital and non-digital media defined within the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, and HHS Information Systems Security and Privacy Policy (IS2P) Appendix I, containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging, and:
1. if hand carried, using a securable container (e.g., locked briefcase) via authorized personnel, or
2. if shipped, trackable with receipt by commercial carrier.
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

Systems processing, storing, or transmitting PII (to include PHI):

The organization protects and controls digital media that contains personally identifiable information (PII) during transport outside of controlled areas using FIPS-validated encryption.

Systems processing, storing, or transmitting PHI:

The organization protects and controls digital media that contains protected health information (PHI) during transport outside of controlled areas using a FIPS 140-2 validated cryptographic module operating in the FIPS-approved mode of operation.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Protect and control non-digital PII/PHI media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. Non-digital PII must be in locked cabinets or sealed packing cartons while in transit.

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs protect and control magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas; and during transport CSPs encrypt digital media using a FIPS 140-2 validated module.
CSP.2 - CSPs define security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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, E-readers), 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Protecting and controlling media containing sensitive information, such as PII, commensurate with the sensitivity of the information contained on the media, during transport outside of controlled areas, promotes accountability and limits situations that make the media vulnerable to unauthorized use and disclosure through loss, theft, or other mishandling.

Reference(s):	**Related Controls Requirement(s):** AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; system 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; and other relevant documents or records.
Interview: Organizational personnel with information system media transport responsibilities.

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Rosters or list of authorized personnel to protect and control PII media during transit.

MP-5(3)	Non-Mandatory: Custodians	P3

Control:

The organization employs an identified custodian during transport of information system media outside of controlled areas.

Supplemental Guidance:

Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another if an unambiguous custodian is always identified.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; information system media transport records; audit records; and other relevant documents or records.
Interview: Organizational personnel with information system media transport responsibilities.

MP-5(4)	Cryptographic Protection (High, Moderate)	P1

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.

Supplemental Guidance:

This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Encrypting portable media and mobile devices protects confidentiality and integrity of sensitive information, such as personally identifiable information (PII), stored on those devices.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. However, using cryptographic protection allows the organization to utilize the “Safe Harbor” provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media if they wish to take advantage of the Safe Harbor provision.

Reference(s): FedRAMP Rev. 4 Baseline; 45 C.F.R. §164.312(a)(2)(iv)	**Related Controls Requirement(s):** MP-2, CP-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media transport; information system media transport records; audit records; and other relevant documents or records.
Test: Cryptographic mechanisms protecting information during transportation outside controlled areas.

MP-6	Media Sanitization (High, Moderate, Low)	P1

Control:

The organization, in accordance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, and HHS IS2P Appendix I:
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.

Systems processing, storing, or transmitting PII (to include PHI):

The organization sanitizes digital media that contains personally identifiable information (PII) prior to disposal, release out of organizational control, or release for reuse using FIPS-validated media sanitization techniques or procedures in accordance with applicable federal and organizational standards and policies.

Systems processing, storing, or transmitting PHI:

The organization sanitizes digital media that contains protected health information (PHI) prior to disposal, release out of organizational control, or release for reuse using FIPS-validated media sanitization techniques or procedures in accordance with applicable federal and organizational standards and policies.

Systems defined as CSPs:

For CSPs, the hypervisor enforces sanitization of the instance (container) image file space upon release:
- Sanitization of released space is compliant with NIST SP 800-88, as amended, guidance.

Implementation Standards:

High & Moderate:

Std.1 - Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.
Std.2 - Surplus equipment is stored securely while not in use, and disposed of or sanitized in accordance with NIST 800-88 when no longer required.

Low:

Std.1 - Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - CSPs support the capability to sanitize disk space when released from an instance (container) image file.
- Sanitization is in accordance with NIST SP 800-88, as amended.

Supplemental Guidance:

This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether 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, 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. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Properly sanitizing media that contains sensitive information, such as PII, prior to disposal or release protects the information from unauthorized use and disclosure.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.310(d)(2)(iii), 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(d)(2)(ii); NIST SP: 800-60, 800-88; Web: nsa.gov/ia/mitigation guidance/	**Related Controls Requirement(s):** MA-2, MA-4, RA-3, SC-4, DM-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; and other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

Systems processing, storing, or transmitting PII (to include PHI):

Examine: PII inventory tape/cartridge log.

MP-6(1)	Review/Approve/Track/Document/Verify (High)	P1

Control:

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Tracking, documenting, and verifying media sanitization and disposal actions for media that contains sensitive information, such as personally identifiable information (PII), reduces the risk of unauthorized disclosure of sensitive information and increases accountability.

Reference(s): FIPS Pub: 199; NIST SP: 800-60, 800-88; 45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.312(d)(2)(ii)	**Related Controls Requirement(s):** SI-12, DM-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records, audit records, and other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

Systems processing, storing, or transmitting PII (to include PHI):

Examine: PII inventory tape/cartridge log.

MP-6(2)	Equipment Testing (High)	P1

Control:

The organization tests sanitization equipment and procedures within every three hundred sixty-five (365) days to verify that the intended sanitization is being achieved.

Supplemental 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).

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 199; NIST SP: 800-60, 800-88	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

MP-6(3)	Nondestructive Techniques (High)	P1

Control:

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances:
a. Prior to initial use after purchase;
b. When obtained from an unknown source;
c. When the organization loses a positive chain of custody; and
d. When device was connected to a lower assurance network/system based on FIPS 199 security categorization.

Supplemental Guidance:

This control enhancement applies to digital media containing Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning portable storage devices for malicious code is recommended, sanitization provides additional assurance that the devices are free of malicious code, including code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices.

Reference(s): FIPS Pub: 199; NIST SP: 800-60, 800-88	**Related Controls Requirement(s):** SI-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; and other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

MP-6(8)	Non-Mandatory: Remote Purging/Wiping of Information	P3

Control:

The organization provides the capability to purge/wipe information from information systems, system components, and devices either remotely or as defined in the RMH standards and procedures.

Supplemental Guidance:

This control enhancement protects data/information on organizational information systems, system components, or devices (e.g., mobile devices) if such systems, components, or devices are obtained by unauthorized individuals. Remote purge/wipe commands require strong authentication to mitigate the risk of unauthorized individuals purging/wiping the system/component/device. The purge/wipe function can be implemented in a variety of ways including, for example, by overwriting data/information multiple times or by destroying the key necessary to decrypt encrypted data.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Organizations must consider the use of this control for moderate and high personally identifiable information (PII) confidentiality impact level information on devices such as mobile devices like an iPad or other smart device. If your organization permits use of personal smart devices (for example, Bring Your Own Device [BYOD]), the organization must evaluate methods to ensure this control is enforced or that compensating controls are in place.

Reference(s): FIPS Pub: 199; NIST SP: 800-60, 800-88	**Related Controls Requirement(s):** DM-2, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization:

(i) Defines information systems, system components, or devices to purge/wipe either remotely or under specific organizational conditions;
(ii) Defines conditions under which information is to be purged/wiped from organization-defined information systems, system components, or devices; and
(iii) Provides the capability to purge/wipe information from organization-defined information systems, system components, or devices either:
(a) Remotely; or
(b) Under organization-defined conditions.

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; information system design documentation; information system configuration settings and associated documentation; media sanitization records; audit records; and 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 purging/wiping media; automated mechanisms supporting and/or implementing purge/wipe capabilities.

MP-7	Media Use (High, Moderate, Low)	P1

Control:

The organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards in accordance with CMS organizational policy and HHS IS2P Appendix I.

Systems processing, storing, or transmitting PII (to include PHI):

The organization restricts the use of portable storage and mobile devices on information systems and networks containing personally identifiable information (PII), without using device ownership, media sanitization and encryption controls.

Supplemental 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, 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control applies to devices containing PII, particularly portable storage and mobile devices.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 199; HHS: IS2P 2014; NIST SP: 800-111	**Related Controls Requirement(s):** AC-19, PL-4, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media usage; information system audit records; and other relevant documents or records.
Examine: Information system restricts the use of portable storage devices.
Interview: Organizational personnel with information system media responsibilities; organizational personnel on use of personally owned media.
Test: Automated mechanisms implementing restrictions on the use of non-organizationally owned media.

MP-7(1)	Prohibit Use Without Owner (High, Moderate)	P1

Control:

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Supplemental 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).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The ability to identify the owner of removable media that stores sensitive information, such as personally identifiable information (PII), assigns accountability and responsibility managing the media and responding to a privacy breach.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-111	**Related Controls Requirement(s):** PL-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media usage; information system audit records; and other relevant documents or records.
Examine: Information system prohibits the use of portable storage devices when there is no identifiable device owner.
Interview: Organizational personnel with information system media responsibilities; organizational personnel on use of portable storage devices.
Test: Automated mechanisms implementing restrictions on the use of portable storage devices.

MP-CMS-1	Media Related Records (High, Moderate)	P2

Control:

Inventory and disposition records for information system media must be maintained to ensure control and accountability of sensitive information. The media related records must contain sufficient information to reconstruct the data in the event of a breach.

Implementation Standards:

High & Moderate:

Std.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.

Supplemental Guidance:

This control addresses management of media used in the operation and maintenance of an information system that processes, stores, or transmits sensitive information such as PII or PHI. Managing media includes both maintaining an accurate inventory and monitoring the media while in use. Finally, management requires creation of disposition records when the media is no longer associated with the system. This ensures control and accountability of the sensitive information stored on the media.

Reference(s): OMB Memo: M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information system media protection policy; procedures addressing media handling, ownership, and disposal; media sanitization records, audit records, and other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities

B.11 Physical and Environmental Protection (PE)

PE-1	Physical and Environmental Protection Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

b. Reviews and updates (as necessary) the current:

1. Physical and environmental protection policy within every three (3) years; and

2. Physical and environmental protection procedures within every three (3) years.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PHI:

Sensitivity of PHI may impact the necessary physical and environmental controls. Physical controls are important for protecting PHI against unauthorized access, use, and disclosure. Environmental controls can be critical when PHI has high availability requirements (e.g., core mission capabilities of an organization rely on consistent and frequent access to PHI).

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(a)(2)(ii), 45 C.F.R. §164.310(a)(2)(iii); NIST SP: 800-12, 800-100	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy and procedures; and other relevant documents or records.

Interview: Organizational personnel with physical and environmental protection responsibilities.

PE-2	Physical Access Authorizations (High, Moderate, Low)	P1

Control:

The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b. Issues authorization credentials for facility access;

c. Reviews the access list detailing authorized facility access by individuals every (90 High, 180 Moderate, 365 Low) days; and

d. Removes individuals from the facility access list when access is no longer required.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization reviews and approves the access list and authorization credentials at least every 365 days, removing from the access list personnel no longer requiring access.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. Maintaining a current list of personnel that are authorized to access facilities where sensitive information is located protects the information from unauthorized access. For the purposes of this control, "sensitive information" includes personally identifiable information (PII) and protected health information.

Reference(s): Code: 5 U.S.C. §552a(b), (e)(10)164.310(a)(2)(iii); FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii) OMB Circular A-130: 7.g	**Related Controls Requirement(s):** PE-3, PE-4, PS-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.

PE-2(1)	Non-Mandatory: Access by Position/Role	P3

Control:

The organization authorizes physical access to the facility where the information system resides based on position or role.

Supplemental Guidance:

Implementing role-based access controls for physical access provides a further level of granularity in governing who can access facilities, and even certain parts of facilities, that store and process sensitive information.

Guidance for systems processing, storing, or transmitting PHI:

The authorization of physical access to the facility should include considerations of whether the person needs access to PHI and whether such access is permitted under the HIPAA Security Rule.

Reference(s): 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(iii)	**Related Controls Requirement(s):** AC-2, AC-3, AC-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PHI:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; 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.
Interview: Organizational personnel with physical access authorization responsibilities; 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.

PE-3	Physical Access Control (High, Moderate, Low)	P1

Control:

The organization:
a. Enforces physical access authorizations at defined entry/exit points to the facility (defined in the applicable security plan) where the information system resides by;
1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan).
b. Maintains physical access audit logs for defined entry/exit points (defined in the applicable security plan);
c. Provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan);
e. Secures keys, combinations, and other physical access devices;
f. Inventories defined physical access devices (defined in the applicable security plan) no less often than every (90 High, 90 Moderate, or 180 Low) days; and
g. Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every 365 days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Implementation Standards:

High & Moderate:

Std.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.
Std.2 - Store and operate servers in physically secure environments and grant access to explicitly authorized personnel only. Access is monitored and recorded.
Std.3 - Restrict access to grounds/facilities to authorized persons only.

Low:

Std.1 - Control data center/facility access by use of door and window locks.
Std.2 - Store and operate servers in physically secure environments protected from unauthorized access.

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.
PRIV.2 - Require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access afterhours.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization inventories physical access devices at least every 365 days.

Supplemental 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. The Federal Identity, Credential, and Access Management (FICAM) Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. 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 in areas designated as publicly accessible with organizations safeguarding access to such devices.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Employing physical access controls that limit access to a facility that are commensurate with the level of sensitivity of the information processed in a facility protects the information from unauthorized access, use, and disclosure.

Reference(s): Code: , 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; FIPS Pub: 201; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(c); NIST SP: 800-73, 800-76, 800-78, 800-116; OMB Circular A-130: 7.g; Web: fips201ep.cio.gov, idmanagement.gov	**Related Controls Requirement(s):** AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; records of key and lock combination changes; storage locations for physical access devices; and other relevant documents or records.

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Restricted areas, security rooms, or locked rooms that control access to areas containing PII.
Interview: Organization personnel responsible for controlling restricted areas, security rooms, or locked rooms containing PII.
Examine: PII protection barriers.
Interview: Organizational personnel with physical access control responsibilities.

PE-3(1)	Information System Access (High)	P1

Control:

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.).

Supplemental Guidance:

This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers).

Reference(s):	**Related Controls Requirement(s):** PS-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; and other relevant documents or records.

PE-4	Access Control for Transmission Medium (High, Moderate)	P1

Control:

The organization controls physical access to telephone closets and information system distribution and transmission lines within organizational facilities using defined security safeguards (defined in the applicable security plan).

Implementation Standards:

High & Moderate:

Std.1 - Disable any physical ports (e.g., wiring closets, patch panels, etc.) not in use.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PHI:

Protecting physical access to transmission medium protects the confidentiality of PHI by protecting it from eavesdropping, the integrity of PHI by protecting it from modification (when unencrypted), and protects the availability of PHI by helping to prevent accidental or intentional damage or disruption to transmission lines.
Under the HIPAA Security Rule, this is an addressable implementation specification.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.310(c)	**Related Controls Requirement(s):** MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.

PE-5	Access Control for Output Devices (High, Moderate)	P2

Control:

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The access controls applied to output devices should be commensurate with the personally identifiable information (PII) confidentiality impact level. For example, human resource information is only sent to printers located in secured locations such as a locked suite.

Reference(s): Code: 5 U.S.C. §552a(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(b), 164.310(c); OMB Circular A-130: 7.g	**Related Controls Requirement(s):** PE-2, PE-3, PE-4, PE-18

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information system restricts the use of unapproved output devices.
Interview: Organizational personnel on physical access to information system output devices.
Test: Automated mechanisms implementing restrictions on connecting unapproved output devices.

PE-6	Monitoring Physical Access (High, Moderate, Low)	Assurance	P1

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 or indications of potential events involving physical security; and
c. Coordinates results of reviews and investigations with the organization's incident response capability.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization reviews physical access logs at least semi-annually.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PHI:

Monitoring physical security incidents could identify PHI incidents or breaches.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.308(a)(6)(i)	**Related Controls Requirement(s):** CA-7, IR-4, IR-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical access logs or records; and other relevant documents or records.
Interview: Organizational personnel with physical access monitoring responsibilities.

PE-6(1)	Intrusion Alarms/Surveillance Equipment (High, Moderate)	Assurance	P1

Control:

The organization monitors physical intrusion alarms and surveillance equipment.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; and other relevant documents or records.
Interview: Organizational personnel with physical access monitoring responsibilities.
Test: Physical access monitoring capability.

PE-6(4)	Monitoring Physical Access to Information Systems (High)	Assurance	P1

Control:

The organization monitors physical access to the information system, in addition to the physical access monitoring of the facility, at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.).

Supplemental Guidance:

This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers).

Reference(s):	**Related Controls Requirement(s):** PS-2, PS-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; and other relevant documents or records.
Interview: Organizational personnel with physical access monitoring responsibilities.

PE-8	Visitor Access Records (High, Moderate, Low)	Assurance	P3

Control:

The organization:
a. Maintains visitor access records to the facility where the information system resides for two (2) years; and
b. Reviews visitor access records no less often than monthly.

Implementation Standards:

High, Moderate, & Low:

Std.1 - At a minimum, visitor access records must include the following information:
1. Name and organization of the person visiting;
2. Visitor's signature;
3. Form of identification;
4. Date of access;
5. Time of entry and departure;
6. Purpose of visit; and
7. Name and organization of person visited.

Supplemental 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. See NARA Schedule 18 for additional detail on this requirement.

Guidance for systems processing, storing, or transmitting PHI:

Visitor access records provide a history of who had access to facilities in the event of a privacy incident or breach. Records should be retained in accordance with the organization's records retention schedule

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for reviewing physical access records.

PE-8(1)	Automated Records Maintenance/Review (High)	P3

Control:

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

Supplemental Guidance:

None.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing facility access records; automated mechanisms supporting management of access records; facility access control logs or records; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for reviewing physical access records.

PE-9	Power Equipment and Cabling (High, Moderate)	P1

Control:

The organization protects power equipment and power cabling for the information system from damage and destruction.

Implementation Standards:

High & Moderate:

Std.1 - Permit only authorized maintenance personnel to access infrastructure assets, including power generators, heating, ventilation, and air conditioning (HVAC) systems, cabling, and wiring closets.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	Related Controls Requirement(s): PE-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; and other relevant documents or records.

PE-10	Emergency Shutoff (High, Moderate)	P1

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.

Implementation Standards:

High & Moderate:

Std.1 - Implements and maintains a master power switch or emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms.

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization defines emergency shutoff switch locations. The locations are approved and accepted by the Joint Authorization Board (JAB).

Supplemental Guidance:

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

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	**Related Controls Requirement(s):** PE-15

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; and other relevant documents or records.

PE-11	Emergency Power (High, Moderate)	P1

Control:

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to a long-term alternate power source in the event of a primary power source loss.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	**Related Controls Requirement(s):** AT-3, CP-2, CP-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; and other relevant documents or records.
Test: Uninterruptible power supply.

PE-11(1)	Long-Term Alternate Power Supply - Minimal Operational Capability (High)	P1

Control:

The organization provides a long-term alternate power supply for the information system that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Implementation Standards:

High:

Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.

Supplemental Guidance:

This control enhancement can be satisfied, for example, using a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; and other relevant documents or records.
Test: Alternate power supply.

PE-12	Emergency Lighting (High, Moderate, Low)	P1

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.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.

Supplemental Guidance:

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

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	Related Controls Requirement(s): CP-2, CP-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Interview: Organizational personnel with emergency planning responsibilities.
Test: Emergency lighting capability.

PE-13	Fire Protection (High, Moderate, Low)	P1

Control:

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.

Supplemental 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 devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.

PE-13(1)	Detection Devices/Systems (High)	P1

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 or safety plan) in the event of a fire.

Supplemental Guidance:

Organizations can identify specific personnel, roles, and emergency responders if 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.

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 devices/systems; fire suppression and detection devices/systems documentation; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.
Test: Simulated activation of fire detection devices/systems and automated notifications.

PE-13(2)	Suppression Devices/Systems (High)	P1

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 (defined in the applicable security or safety plan).

Supplemental Guidance:

Organizations can identify specific personnel, roles, and emergency responders if 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.
Test: Simulated activation of fire suppression devices/systems and automated notifications.

PE-13(3)	Automatic Fire Suppression (High, Moderate)	P1

Control:

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

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

PE-14	Temperature and Humidity Controls (High, Moderate, Low)	P1

Control:

The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-specified levels;
b. Monitors temperature and humidity levels within the defined frequency (defined in the applicable security plan); and
c. Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.

Implementation Standards:

High & Moderate:

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

Low:

Std.1 - Evaluate the level of alert and follow prescribed guidelines for that alert level.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - CSPs must implement this Standard (PE-14 CSP.1) as a replacement for the above Control (PE-14). The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides at levels consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled “Thermal Guidelines for Data Processing Environments”; and
b. Monitors temperature and humidity levels continuously.
CSP.2 - For CSPs, the organization measures temperature at server inlets and humidity levels by dew point.

Supplemental Guidance:

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

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	**Related Controls Requirement(s):** AT-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; security plan; temperature and humidity controls; facility housing the information system; temperature and humidity controls documentation; temperature and humidity records; and other relevant documents or records.
Interview: Organization personnel with physical and environmental protection responsibilities.
Test: Simulated activation of fire suppression devices/systems and automated notifications.

PE-15	Water Damage Protection (High, Moderate, Low)	P1

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.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	**Related Controls Requirement(s):** AT-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; 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; and other relevant documents or records.
Interview: Organization personnel with physical and environmental protection responsibilities.
Test: Master water-shutoff valves; process for activating master water-shutoff.

PE-15(1)	Automation Support (High)	P1

Control:

The organization employs automated mechanisms to detect the presence of water near the information system and alerts defined personnel or roles (defined in the applicable security plan).

Implementation Standards:

High:

Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.

Supplemental Guidance:

Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; automated mechanisms for water shutoff valves; and other relevant documents or records.
Test: Automated mechanisms implementing master water shutoff valve activation.

PE-16	Delivery and Removal (High, Moderate, Low)	P2

Control:

The organization authorizes, monitors, and controls the flow of all information system-related components entering and exiting the facility and maintains records of those items.

Implementation Standards:

Systems defined as CSPs:

High, Moderate. & Low:

CSP.1 - CSPs must implement this Standard (PE-16 CSP.1) as a replacement for the above Control (PE-16). The organization authorizes, monitors, and controls the flow of all information system components entering and exiting the facility and maintains records of those items.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2	**Related Controls Requirement(s):** CM-3, MA-2, MA-3, MP-5, SA-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; security plan; facility housing the information system; records of items entering and exiting the facility; and other relevant documents or records.
Interview: Organization personnel with responsibilities for controlling information system components entering and exiting the facility.

PE-17	Alternate Work Site (High, Moderate)	P2

Control:

The organization:
a. Employs appropriate security controls at alternate work sites to include, but not to be limited to, requiring the use of 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:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization defines management, operational, and technical information system security controls for alternate work sites. The security controls are approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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. This control supports the contingency planning activities of organizations and the federal telework initiative.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When personally identifiable information (PII) collected, stored, and processed at an alternate worksite, the information is subject to the same laws, regulations, and policies as PII handled at "non-alternate facilities."

Reference(s): FISCAM: AS-5, CP-2; FedRAMP Rev. 4 Baseline; HIPAA: 45 C.F.R. §164.310(a)(2)(i); NIST SP: 800-46 OMB Memo: M-11-27, M-17-12, Att. 1 and Att. 4	**Related Controls Requirement(s):** AC-17, CP-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Interview: Organization personnel using alternate work sites.

PE-18	Location of Information System Components (High)	P3

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.

Supplemental 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 near information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., using wireless sniffers or microphones).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control is required to limit intentional and unintentional disclosures of personally identifiable information (PII). One example of positioning information system components to minimize the opportunity for unauthorized access would be ensuring that monitors are placed in such a way as to prevent unauthorized viewing. An example of positioning information system components to minimize potential damage from physical land environmental hazards would be to place servers and disk arrays in locations that are secured.

Guidance for systems processing, storing, or transmitting PHI:

This control is required to limit intentional and unintentional disclosures of PHI in violation of the HIPAA Privacy and Security Rules.

Reference(s): Code: 5 U.S.C. §552a(e)(10); FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.310(c); 45 C.F.R. §164.308(a)(3)(i)	**Related Controls Requirement(s):** CP-2, PE-19, RA-3

ASSESSMENT PROCEDURE
Assessment Objective: Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s). **Assessment Methods and Objects:** **Examine:** Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; and other relevant documents or records.

PE-18(1)	Non-Mandatory: Facility Site	P3
Control: The organization plans the location or site of the facility where the information system resides considering physical and environmental hazards associated with existing facilities and considers the physical and environmental hazards in its risk mitigation strategy.		
Supplemental Guidance: None.		
Reference(s):	**Related Controls Requirement(s):** PM-8	
ASSESSMENT PROCEDURE		
Assessment Objective: Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s). **Assessment Methods and Objects:** **Examine:** Physical and environmental protection policy; physical site planning documents; organizational assessment of risk, contingency plan; and other relevant documents or records. **Interview:** Organization personnel with site selection responsibilities for the facility housing the information system.		

B.12 Planning (PL)

PL-1	Security Planning Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:
1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls.
b. Reviews and updates (as necessary) the current:
1. Security planning policy within every three (3) years; and
2. Security planning procedures within every three (3) years.

Systems processing, storing, or transmitting PHI:

The organization retains the policies and procedures in written form (which may be electronic) for 6 years from the date of its creation or the date when it was last in effect, whichever is later. The organization makes the documentation available to those persons responsible for implementing the procedures to which the document pertains.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PHI:

Security planning addresses the requirements for confidentiality, availability, and integrity for the organization and individual information system(s).

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(i); 45 C.F.R. §164.316(b)(2)(ii) HSPD 7: J(35); NIST SP: 800-12, 800-18, 800-100	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Security planning policy and procedures; and other relevant documents or records.
Interview: Organizational personnel with security planning responsibilities.

PL-2	System Security Plan (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops a security plan for the information system that is consistent with the RMH Procedures; and
1. Is consistent with the organization's enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
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 and supplementation 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; and
d. Updates the plan, minimally every three (3) years, to address current conditions or whenever:
- There are significant changes to the information system/environment of operation that affect security;
- Problems are identified during plan implementation or security control assessments;
- When the data sensitivity level increases;
- After a serious security violation caused by changes in the threat environment; or
- Before the previous security authorization expires.
e. Protects the security plan from unauthorized disclosure and modification.

Systems processing, storing, or transmitting PII (to include PHI):

The system security plan (SSP) must provide the security category and the personally identifiable information (PII) confidentiality impact level of the system (as described in NIST SP 800-122), describe relationships with, and data flows of, PII to other systems; and provide an overview of security and privacy requirements for the system. The SSP must define the boundary within the system where PII is stored, processed, and/or maintained. The person responsible for meeting information system privacy requirements must provide input to the SSP.

Systems defined as CSPs:

The associated security plan must address gaps between the FedRAMP baseline and the ARS/CMS Minimum Security Requirements (CMSR) required baseline.

Implementation Standards:

Systems processing, storing, or transmitting PHI:

PHI.1 - Retain documentation of policies and procedures relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b)).

Supplemental Guidance:

Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, 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 Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in NIST 800-53 Appendix D and Committee on National Security Systems (CNSS) Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). NIST 800-53 Appendix I provides guidance on developing overlays.
Security plans need not be single documents; the plans can be a collection of various documents, including documents that already exist. 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 needs to be accomplished by those plans.
All CMS information systems and major applications are covered by a security plan, which is compliant with current CMS procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The SSP is necessary for the information system to be authorized. As the security controls section of a privacy impact assessment or other privacy documentation may not provide sufficient details to determine which controls have been implemented, the SSP and plan of action and milestones (POA&M, see PM-4) are the best locations to address privacy related security controls.

Reference(s): E-Government Act of 2002 (Pub. L. No. 107-347) §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1; HIPAA: 45 C.F.R. §164.306(a); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.310; 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii) HSPD 7: J(35); NIST SP: 800-18; OMB Memo: M-03-22, M-17-12 Att. 1, A.2	**Related Controls Requirement(s):** AC-2, AC-6, AC-14, AC- 17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-4, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Interview: Organization personnel with security planning and plan implementation responsibilities for the information system.

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Procedures that document who obtains documentation and to whom documentation pertains for implementation.
Interview: Organizational personnel who are responsible for implementation of procedures to determine if documentation is available.

Systems processing, storing, or transmitting PHI:

Examine: Sampling of policies and procedures relating to 164.306 for retention period. (See HIPAA 164.316(b))
Interview: Organizational personnel with retention responsibilities related to 164.306. (See HIPAA 164.316(b))

PL-2(3)	Plan/Coordinate with Other Organizational Entities (High, Moderate)	Assurance	P1

Control:

The organization plans and coordinates security-related activities affecting the information system with affected internal or external stakeholders, groups, or organizations before conducting such activities to reduce the impact on other organizational entities.

Supplemental Guidance:

These stakeholders, groups, or organizations could include those involved with security-related activities, or providing services or support (such as [TIC] or those involved in COOP planning).
Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Planning and coordination includes emergency and nonemergency (i.e., planned or non-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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** CP-4, IR-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Interview: Organization personnel with security planning and plan implementation responsibilities for the information system.

PL-4	Rules of Behavior (High, Moderate, Low)	Assurance	P2

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 regarding information and information system usage, including:
i. The HHS RoB and Policy for Personal Use of Information Technology Resources; and
ii. Any applicable CMS RoB; and
iii. Any applicable system-specific RoB.
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 and updates the rules of behavior every three (3) years
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 and at least every 365 days;
e. Informs employees and contractors that the use of CMS information resources for anything other than authorized purposes set forth in the HHS RoB and Policy for Personal Use of Information Technology Resources is a violation of either or both of those policies, and is grounds for disciplinary action, monetary fines, and/or criminal charges that could result in imprisonment; and
f. Informs employees and contractors that the use of CMS information resources is subject to the HHS Policy for Monitoring Employee Use of HHS IT Resources; and
g. In addition to the HHS RoB, the organization may define a system-level RoB acknowledgement.

Systems processing, storing, or transmitting PII (to include PHI):

Pursuant to OMB M-17-12, organizational rules of behavior must include a policy outlining the rules of behavior to safeguard personally identifiable information (PII) and identifying consequences and corrective actions for failure to follow these rules. Consequences should be commensurate with level of responsibility and type of PII involved.

Supplemental 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 federal information systems, is often not feasible given the large number of such 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.
Rules of behavior are aligned with HHS requirements and made readily available.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Rules of behavior govern expectations of system users for systems that handle sensitive information such as PII.

Reference(s): Code: 5 U.S.C. §552a(e)(9); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HHS; Policy for Monitoring Employee Use of HHS IT Resources; HSPD 7: J(35); NIST SP: 800-18; OMB Memo: M-17-12, Att. 1, A.2. and Att. 4	**Related Controls Requirement(s):** AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, AR-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 who are authorized users of the information system and have signed rules of behavior

PL-4(1)	Social Media and Networking Restrictions (High, Moderate)	Assurance	P2

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.

Supplemental 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, personally identifiable information) from social media/networking sites.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-18	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 who are authorized users of the information system and have signed rules of behavior.

PL-8	Information Security Architecture (High, Moderate)	Assurance	P1

Control:

The organization:
a. Develops an information security architecture for the information system that:
1. Describes the overall requirements and approach to be taken regarding protecting the confidentiality, integrity, and availability of organizational information;
2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
3. Describes any information security assumptions about, and dependencies on, external services.
b. Reviews and updates (as necessary) the information security architecture no less often than every three (3) years and whenever changes are made to the enterprise architecture;
c. Ensures that planned information security architecture changes are reflected in the security plan and organizational procurements/acquisitions; and
d. Ensures that the planned information security architecture is consistent with the CMS's enterprise architecture program and is based on the taxonomy of the Federal Enterprise Architecture (FEA).

Supplemental Guidance:

This control addresses actions taken by organizations in the design and development of information 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. In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers (to include CSPs). Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business 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 Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) 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 information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The information security architecture identifies security and privacy controls necessary to support privacy requirements. The SAOP or CPO are the best resource for identifying privacy requirements and privacy controls.

Reference(s): Code: 5 U.S.C. §552a(e)(10); E-Government Act of 2002 (Pub. L. 107-347) §208; FedRAMP Rev. 4 Baseline; OMB Memo: M-03-22	**Related Controls Requirement(s):** CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, AR-7, Appendix J

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; and other relevant documents or records.

B.13 Personnel Security (PS)

PS-1	Personnel Security Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

b. Reviews and updates (as necessary) the current:

1. Personnel security policy within three (3) years; and
2. Personnel security procedures within every three (3) years.

Systems processing, storing, or transmitting PII (to include PHI):

The personnel security policies and procedures must address the different levels of background investigations, or other personnel security requirements, necessary to access different levels of personally identifiable information (PII).

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Roles that require access to certain types of sensitive information, such as PII may require additional personnel security measures beyond those applied to the general workforce of an organization.

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3, SM-4; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii) NIST SP: 800-12, 800-100; OMB Memo: M-17-12, Att. 4; OMB Circular A-130: 7.g. and 8.a.1(f)	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Personnel security policy and procedures; and other relevant documents or records.

PS-2	Position Risk Designation (High, Moderate, Low)	P1

Control:

The organization:
a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions;
c. Ensures that all individuals with significant security responsibilities possess, at a minimum, a Tier 2S background investigation;
d. Ensures that individuals are designated to position-sensitivity levels that are commensurate with the responsibilities and risks associated with the position; and
e. Reviews and, if necessary, updates position risk designations at least within three years or whenever a position's duties are changed/revised/realigned, and ensures that these risk designations are consistent with OPM policy and guidance. in accordance with CMS Personnel Security Policy

Systems processing, storing, or transmitting PII (to include PHI):

Whether a member of the workforce will be working with personally identifiable information (PII) is a factor in determining the screening criteria for working in the position.

Supplemental Guidance:

Position risk designations reflect OPM 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, security clearances).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Position risk designations, for different levels of access to sensitive information such as PII should be commensurate with the risks associated with the confidentiality impact level for the information.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s):	**Related Controls Requirement(s):** AT-3, PL-2, PS-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 risk designation reviews and updates; and other relevant documents or records.

PS-3	Personnel Screening (High, Moderate, Low)	P1

Control:

The organization:
a. Screens individuals prior to authorizing access to the information system;
b. Rescreens individuals periodically and anytime they move to a new position with a higher risk designation, in accordance with CMS Personnel Security Policy;
c. Conducts background investigations in a manner commensurate with OPM, HHS, and CMS Personnel Security policy and guidance;
d. Performs reinvestigations for active national security clearances in accordance with guidance provided by current personnel security policy; and
e. Refuses employees and contractors access to information systems until they have:
1. Been vetted in accordance with agency policy; and
2. Signed the appropriate access agreements.

Systems processing, storing, or transmitting PII (to include PHI):

Individuals that work with personally identifiable information (PII) are screened prior to being provided access to the PII and re-screened as determined by the organization.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Require that individuals with significant security responsibilities be assigned and hold, at a minimum, a Tier 2S background investigation as defined in the HHS Personnel Security/Suitability Handbook. Assign other individuals with Public Trust positions the appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - The organization rescreens individuals per the following:
(a) For national security clearances; a reinvestigation is required during the fifth year for top secret security clearance, the tenth year for secret security clearance, and fifteenth year for confidential security clearance; and
(b) For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth year. There is no reinvestigation for other moderate risk positions or any low risk positions.

Supplemental Guidance:

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

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Screening individuals who are provided access to sensitive information, such as PII, and re-screening as deemed appropriate by CMS or the organization, reduces risk.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s):	**Related Controls Requirement(s):** AC-2, IA-4, PE-2, PS-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; and other relevant documents or records.

PS-4	Personnel Termination (High, Moderate, Low)	P2

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 the terminated individual;
f. Notifies defined personnel or roles (defined in the applicable security plan) within one (1) calendar day; and
g. Immediately escorts employees terminated for cause out of the organization.

Implementation Standards:

High & Moderate:

Std.1 - System access must be revoked prior to or during the employee termination process/action.
Std.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).

Low:

Std.1 - System access must be revoked during the employee termination process/action.
Std.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).

Supplemental 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 by being 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 certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.
Appropriate personnel have access to official records created by terminated employees that are stored on information systems.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control governs termination procedures for access to sensitive information, such as personally identifiable information (PII).

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s):	**Related Controls Requirement(s):** AC-2, IA-4, PE-2, PL-4, PS-5, PS-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Human Resources policy; OAGM policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; and other relevant documents or records.

PS-4(2)	Automated Notification (High)	P1

Control:

The organization employs automated mechanisms to notify defined personnel/roles as designated by the organization (e.g., Human Resources, managers/supervisors, system administrators, physical security personnel) upon termination of an individual.

Implementation Standards:

High:

Std.1 - If automated mechanisms are not feasible, a manual and documented process must be in place consistent with the PS-4(f) control.

Supplemental Guidance:

In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications—or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles (e.g., management personnel, supervisors, personnel security officers, information security officers, systems administrators, or information technology administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Human Resources policy; OAGM policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; and other relevant documents or records.
Interview: Organizational personnel with Human Resources responsibilities for employees and CORs with responsibility for contractors.

PS-5	Personnel Transfer (High, Moderate, Low)	P2

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 or confirming the need to continue to have/access appropriate information system-related property (e.g., keys, identification cards, building passes);
2. Notifying security management;
3. Closing obsolete accounts and establishing new accounts; and
4. When an employee moves to a new position of trust, re-evaluating logical and physical access controls as soon as possible but not to exceed 30 days.
c. Modifying access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifying defined personnel or roles (defined in the applicable security plan) within one (1) business day.

Systems processing, storing, or transmitting PII (to include PHI):

Individuals that work with personally identifiable information (PII) are screened prior to being provided access to the PII and re-screened as determined by the organization.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates organization-defined transfer or reassignment actions within five (5) days following the formal transfer action.
CSP.2 - For CSPs, the organization defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the Joint Authorization Board (JAB).

Supplemental Guidance:

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. 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 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When personnel are reassigned or transferred, their access to sensitive information, such as PII, must be reviewed to determine whether and how their access permissions should change.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): Code: 5 U.S.C. §552a(b)(1) and (e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(B)	**Related Controls Requirement(s):** AC-2, IA-4, PE-2, PS-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Human Resources 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 Human Resources responsibilities.

PS-6	Access Agreements (High, Moderate, Low)	Assurance	P3

Control:

The organization:
a. Develops and documents access agreements for organizational information systems;
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 365 days, whichever occurs first; and
c. Ensures that individuals requiring access to organizational information and information systems:
1. Acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and
2. Re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated or within every 365 days.

Supplemental 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.
The HHS RoB is the standard HHS access agreement. All new users of HHS, including CMS, information resources must read the HHS RoB and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed every 365 days thereafter, which may be done as part of annual the organization Information Systems Security Awareness Training (see AT-3).

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Examples of access agreement documents required for access to personally identifiable information (PII) may include access authorization requests, nondisclosure agreements, acceptable use agreements, privacy training and awareness, and rules of behavior.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, AS-4, SD-1, SD-2, SM-4; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(d)(2)(iii), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.314(a) OMB Memo: M-17-12 Att. 1, A.2. and Att. 4	**Related Controls Requirement(s):** AC-2, PL-4, PS-2, PS-3, PS-4, PS-8, AR-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: OIT policy; procedures addressing access agreements for organizational information and information systems; security plan; access agreements; records of access agreement reviews and updates; and other relevant documents or records.
Interview: Organizational personnel with IT security responsibilities.

PS-7	Third-Party Personnel Security (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party (e.g. external, contractor or cloud service provider [CSP]) 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 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 as soon as possible within a maximum of 72 hours for systems designated as High impact; seven calendar days for systems designated as Moderate impact, or 30 calendar days for systems designated as Low impact, from the formal termination action; and
e. Monitors provider compliance.

Implementation Standards:

High, Moderate, & Low:

Std.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.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

This control ensures that third-party service providers (to include CSPs) that will have access to sensitive information, such as personally identifiable information (PII), are held accountable in the same way the organizational personnel are held accountable.

Reference(s): Code: 5 U.S.C. §552a(m); Federal Acquisition Regulation (FAR): Parts 24.1, 39.105, 52.224-1&2; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4, SM-7; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.314(a); NIST SP: 800-35; OMB Circular A-130: 7.g., 8.a.1(f)	**Related Controls Requirement(s):** PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21, AR-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; and other relevant documents or records.
Interview: CORs, personnel security specialists; third-party providers.

PS-8	Personnel Sanctions (High, Moderate, Low)	P3

Control:

The organization:
a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies defined personnel or roles (defined in the applicable security plan) within defined time period (defined in the applicable security plan), not to exceed three calendar days for systems designated as High impact; seven calendar days for systems designated as Moderate impact; and thirty calendar days for systems designated as Low impact when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Supplemental Guidance:

Organizational sanctions processes reflect applicable federal laws, Executive Orders, 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 General Counsel regarding matters of employee sanctions.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

If the personnel sanctions are associated with the loss, theft, or compromise of personally identifiable information (PII), additional care must be taken to prevent further privacy incidents. When providing notice of sanctions, do not provide the PII involved in the incident to anyone without an explicit need to know. Unless the individual needs the specific PII elements breached to perform their job function, the individual does not need to know the PII. Instead, provide characterization of the type(s) of PII breached (e.g., provide “Full Name” instead of providing “John Doe,” or “Blood Type” instead of “A positive”).

Reference(s): Code: 5 U.S.C. §552a(e)(9); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(C); OMB Memo: M-17-12 Att. 2, A.2., Att. 4	**Related Controls Requirement(s):** PL-4, PS-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: OIT policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; and other relevant documents or records.
Interview: Organizational personnel with IT security responsibilities.

B.14 Risk Assessment (RA)

RA-1	Risk Assessment Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls on information systems and paper records; and

b. Reviews and updates (as necessary) the current:

1. Risk assessment policy within every three (3) years and
2. Risk assessment procedures within every three (3) years.

Systems processing, storing, or transmitting PII (to include PHI):

Organization risk assessment policy and procedures must incorporate the requirements to conduct information system privacy risk management processes across the life cycle of an information system collecting, using, maintaining, and/or disseminating personally identifiable information (PII).

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The Privacy Office (Senior Official for Privacy) should be consulted when developing risk assessment policy and procedures to cover information systems containing PII.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.316(a); NIST SP: 800-12, 800-30, 800-100; OMB Circular A-130: 7.g. and 8.b.(3)(b); OMB Memo: M- 17-12 Att. 1, A.2., M-05-08	**Related Controls Requirement(s):** PM-2, PM-9, AR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Risk assessment policy and procedures; and other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.

RA-2	Security Categorization (High, Moderate, Low)	P1

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 security categorization decision is reviewed and approved by the authorizing official or authorizing official's designated representative.

Systems processing, storing, or transmitting PII (to include PHI):

Involve the Senior Official for Privacy, or their designee, when conducting the security categorization process for information systems containing personally identifiable information (PII) or protected health information (PHI).

Supplemental 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 and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives (HSPD), potential national-level adverse impacts. 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 CMS information systems categorized as High or Moderate are considered sensitive or contain sensitive information. All CMS information systems categorized as Low are considered non-sensitive or contain non-sensitive information. Organizations implement the minimum-security requirements and controls as established in the current CMS Information Security ARS Standard, based on the system security categorization.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

A determination of security categorization is based in part on whether the information is PII, or the system contains sensitive information such as PII, and is a fundamental determination for implementing security controls.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AS-1, SM-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(A), 45 C.F.R. §164.308(a)(1)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(E); NIST SP: 800-30, 800-39, 800-60; OMB Memo: M-17-12 Att. 1, A.2, M-06-16, M-14-04	**Related Controls Requirement(s):** CM-8, MP-4, RA-3, SC-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; security plan; security categorization documentation; and other relevant documents or records.
Interview: Organizational personnel with security categorization and risk assessment responsibilities.

RA-3	Risk Assessment (High, Moderate, Low)	Assurance	P1

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. Conducts an E-Authentication Risk Assessment (ERA), as required, on systems and determines e-authentication assurance levels;
c. Documents risk assessment results in the applicable security plan;
d. Reviews risk assessment results within every 365 days;
e. Disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO; and
f. Updates the risk assessment before issuing a new authority to operate (ATO) package or within every three (3) years, whichever comes first; 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.

Systems processing, storing, or transmitting PII (to include PHI):

Include an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of personally identifiable information (PII) in the related risk assessment documentation.

Systems processing, storing, or transmitting PHI:

The organization documents risk assessment results in a HIPAA Risk Analysis, and associated risks to PHI must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings. All HIPAA Risk Analysis documentation must be maintained for 6 years from the date of creation or date it was last in effect – whichever is later.

Implementation Standards:

Systems defined as CSPs:

High, Moderate & Low:

CSP.1 - For CSPs, the organization documents risk assessment results in the security assessment report.

CSP.2 - For CSPs, the organization reviews risk assessment results at least every three (3) years or when a significant change occurs.

Supplemental Guidance:

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments consider 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 consider risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.

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, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

A standardized risk assessment process should include a consideration of risks associated with the collection, maintenance, and use of sensitive information such as PII. Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. An evaluation of privacy risk for an information system benefits an organization and the individuals whose PII are included by enabling the organization to identify, evaluate, and manage the privacy risks for the information in that system. The content of the privacy risk assessment performed under this control should be addressed in concert with the privacy risk evaluation conducted through the internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing privacy-related sensitive information.

A standardized risk assessment process should include a consideration of risks associated with the collection, maintenance, and use of sensitive information such as PII. An evaluation of risks associated with the potential impact of loss of the PII must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings. Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. An evaluation of privacy risk for an information system benefits an organization and the individuals whose PII are included by enabling the organization to identify, evaluate, and manage the privacy risks for the information in that system. The content of the privacy risk assessment performed under this control should be addressed in concert with the privacy risk evaluation conducted through the internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing privacy-related sensitive information.

Guidance for systems processing, storing, or transmitting PHI:

The Department of Health and Human Services has issued Final Guidance on Risk Analysis (Assessment) under the HIPAA Security Rule (see http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf).

Reference(s):	**Related Controls Requirement(s):** RA-2, PM-9, AR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization has implemented all elements of this control as described in the PII control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; system security plan; risk assessment; and other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.

RA-5	Vulnerability Scanning (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Scans for vulnerabilities in the information system and hosted applications no less often than once every 72 hours 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;
4. Complying with DHS Continuous Diagnostics and Mitigation program and CMS requirements; and
5. Complying with required reporting metrics (e.g., CyberScope).
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates vulnerabilities based on the Business Owner's risk prioritization in accordance with the guidance defined under security control SI-02; 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).

Systems defined as CSPs:

This control requirement replaces RA-05(a.):
a. Scans for vulnerabilities in the information system and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the system/applications are identified and reported.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Vulnerability scans must be performed when new vulnerabilities, risks, or threats potentially affecting the system/applications are identified and reported or upon request from CMS.
Std.2 - Vulnerability scanning tools results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Vulnerability scan information sources include systems, appliances, devices, services, and applications (including databases); and
(c) CCIC directed vulnerability scan information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.3 - As required by CMS, raw results from vulnerability scanning tools must be available in an unaltered format to the CCIC.
Std.4 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational monitoring status and security posture information.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization scans for vulnerabilities in the information system and hosted applications as required under DHS Continuous Diagnostics and Mitigation and NIST Continuous Monitoring guidelines for CSPs; and operating system, web application, and database scans (as applicable); and when new vulnerabilities potentially affecting the system/applications are identified and reported.
CSP.2 - For CSPs, the organization remediates vulnerabilities based on the Business Owner's risk prioritization in accordance with the guidance defined under security control SI-02. Use of time periods that exceed CMS standards but are approved and accepted by the Joint Authorization Board (JAB) must be authorized by the CISO

Supplemental 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, 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 which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).
The organization remediates vulnerabilities based on the Business Owner's risk prioritization in accordance with the guidance defined under security control SI-02. Penetration testing is covered under CA-08.
Contact your CRA or the CCIC for the list of compliant formats.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, AS-3, CM-5, SM-5; HSPD 7: F(19), G(24); NIST SP: 800-37, 800-39, 800-40, 800-70, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; Web: cwe.mitre.org, nvd.nist.gov	**Related Controls Requirement(s):** CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; vulnerability scanning results; patch and vulnerability management records; and other relevant documents or records.
Examine: Information system capabilities to confirm the system can perform an on-demand custom vulnerability assessment. The assessment capability must support an on- demand (manually initiated) vulnerability scan with predefined or custom content.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.

RA-5(1)	Update Tool Capability (High, Moderate)	Assurance	P1

Control:

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

Supplemental Guidance:

The vulnerabilities to be scanned need to be readily updated 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.
The assessment capability must support updates that include predefined or custom content (i.e., meet Continuous Diagnostics and Mitigation required formats and updating frequencies) and provide the capability to update assessment content.

Reference(s): FedRAMP Rev. 4 Baseline; HSPD 7: F(19), G(24) NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** SI-3, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; records of updates to vulnerabilities scanned; and other relevant documents or records.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.
Test: Vulnerability scanning capability and associated scanning tools.

RA-5(2)	Update by Frequency/Prior to New Scan/When Identified (High, Moderate)	Assurance	P1

Control:

The organization updates the database of known information system vulnerabilities to be used in the scanning process no less often than every 72 hours, immediately prior to a new scan, and when new vulnerabilities are identified and reported.

Systems defined as CSPs:

For CSPs, this Standard replaces the requirement defined within RA-05(02). The organization updates the list of information system vulnerabilities scanned no less often than before each scan.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline; HSPD 7: F(19), G(24) NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** SI-3, SI-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; and other relevant documents or records.
Examine: Information system updates vulnerability scanning data as required.

RA-5(4)	Discoverable Information (High)	Assurance	P1

Control:

The organization determines what information about the information system is discoverable by adversaries, and subsequently takes appropriate corrective actions to limit discoverable system information.

Supplemental Guidance:

Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries.

Reference(s): NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** AU-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Risk assessment policy; procedures addressing vulnerability scanning; penetration test results; vulnerability scanning results; and other relevant documents or records.

RA-5(5)	Privileged Access (High, Moderate)	Assurance	P1

Control:

The information system implements privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.

Implementation Standards:

High & Moderate:

Std.1 - Automated scanning tool functionality must be compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements to include the ability to perform credentialed scans.
(a) To the extent possible, credentials will be compliant with CMS policy.
Std.2 - Credentialed scanning must be performed on all information systems and network devices (including appliances).
Std.3 - The organization must maintain and provide changes to the system accounts to support credentialed scanning no later than two (2) weeks prior to expiration or when other changes to the accounts are needed.

Supplemental 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 protects the sensitive nature of such scanning. Privileged access mechanisms must be compliant with CMS requirements for access to elevated privilege accounts. The assessment capability must support use of credentialed scans. Credentialed access is compliant with CMS policy.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.316(a); NIST SP: 800-12, 800-30, 800-37, 800-39, 800-100, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Risk assessment policy; procedures addressing vulnerability scanning; system security plan; list of information system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; and other relevant documents or records.
Examine: Information system provides the capability to perform scans using appropriate credentials.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.

B.15 System and Services Acquisition (SA)

SA-1	System and Services Acquisition Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
b. Reviews and updates (as necessary) the current:
1. System and services acquisition policy within every three (3) years; and
2. System and services acquisition procedures within every three (3) years.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; NIST SP: 800-12, 800-100	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.

SA-2	Allocation of Resources (High, Moderate, Low)	Assurance	P1

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
d. Establishes a discrete line item in CMS's programming and budgeting documentation for the implementation and management of information systems security.

Systems processing, storing, or transmitting PII (to include PHI):

As part of the capital planning and investment control process, the organization must determine, document, and allocate resources required to protect the privacy and confidentiality of personally identifiable information (PII) in the information system.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Resources must be considered for the protection of privacy and confidentiality when budgeting for an information system.

Reference(s): E-Government Act of 2002 (Pub. L. No. 107-347), §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, AS-3, CM-3, SM-1; NIST SP: 800-65; OMB Memo: M-16-04; OMB Circular A-130: 7.g. and 8.b(3)(b)	**Related Controls Requirement(s):** PM-3, PM-11

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; organizational programming and budgeting documentation; other relevant documents or records.
Interview: Organizational personnel with capital planning and investment responsibilities.

SA-3	System Development Life Cycle (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Manages the information system using a formally defined and documented system development life cycle (SDLC) process 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.

Implementation Standards:

High, Moderate, & Low:

Std.1 - The information system must be managed using:
(a) The information security steps of IEEE 12207.0 standard for SDLC, as defined in the CMS eXpedited Life Cycle (XLC), to incorporate information security control considerations; and
(b) The information system architecture defined within the Technical Reference Architecture (TRA).

Supplemental 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 that 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 the development team that 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

To ensure that privacy and security controls are appropriately considered during each phase of the SDLC, both the security and privacy offices should have a clear understanding of the requirements to protect PII. The privacy office should participate throughout the SDLC.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3; NIST SP: 800-37, 800-64; OMB Circular A-130:	Related Controls Requirement(s): AT-3, PM-7, SA-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Interview: Organizational personnel with information security and system life cycle development responsibilities.

SA-4	Acquisition Process (High, Moderate, Low)	Assurance	P1

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; and
g. Acceptance criteria.

Systems processing, storing, or transmitting PII (to include PHI):

When acquiring information systems, components, or services used to store, process, or transmit personally identifiable information (PII), ensure the following, in consultation with the privacy office, are included in the acquisition contract:
a. List of security and privacy controls necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements.
b. Privacy requirements set forth in Appendix J of NIST SP 800-53, Rev. 4, including privacy training and awareness, and rules of behavior.
c. Privacy functional requirements, i.e., functional requirements specific to privacy.
d. Federal Acquisition Regulation (FAR) Clauses per FAR Part 24 (clauses 52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act. and Part 39 (clauses 39.105, Privacy, and 39.116, Contract clause), and any other organization-specific privacy clauses.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Contracts must include the standard CMS information security and privacy contract language.

Systems processing, storing, or transmitting PHI:

PHI.1 - When acquiring information systems, components, or services used to store, process, or transmit PHI, in addition to the requirements for PII, ensure, in consultation with the privacy office, that any necessary memorandum of understanding, memorandum of agreement, and other data sharing agreement are obtained.

Supplemental 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. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include requirements for degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include:
(i) Development processes, procedures, practices, and methodologies; and
(ii) Evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.
Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values using assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services.
Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Contracts for information systems, components, or services must meet the privacy requirements of the Federal Government. It is much easier, and cheaper, to build privacy into a system at the acquisition phase of the life cycle than it is to bolt it on after the system is already acquired.

Reference(s): Code: 5 U.S.C. §552a(m) and (e)(10); E-Government Act of 2002: (I; Pub. L. No. 107-347) §208; FAR: Part 24 and 39.105; Federal Information Management Security Act (Pub. L. No. 107-347); FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; FISCAM: AS-3, CM-3; HIPAA: 164.314(a)(2)(i); NIST SP: 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; OMB Memo: M-16-04; OMB Circular A-130: 7.g. and Appendix 1; Web: acquisition.gov/far, fips201ep.cio.gov, niap-ccevs.org; 45 C.F.R. §164.314(a)	**Related Controls Requirement(s):** CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12, AR-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.

SA-4(1)	Functional Properties of Security Controls (High, Moderate)	Assurance	P1

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.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):** SA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 systems or services; other relevant documents or records.

SA-4(2)	Design/Implementation Information for Security Controls (High, Moderate)	Assurance	P1

Control:

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes:
a. Security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces;
b. Source code and hardware schematics; and
c. High-level design documentation at sufficient detail to prove the security control implementation.

Supplemental 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 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** SA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 systems or services; other relevant documents or records.

SA-4(9)	Functions/Ports/Protocols/Services in Use (High, Moderate)	Assurance	P1

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.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	**Related Controls Requirement(s):** CM-7, SA-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 systems or services; other relevant documents or records.
Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities

SA-4(10)	Use of Approved PIV Products (High, Moderate, Low)	Assurance	P1

Control:

The organization employs only information technology products on the FIPS 201-approved products list for PIV capability implemented within organizational information systems.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** IA-2, IA-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 systems or services; other relevant documents or records.
Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.

SA-5	Information System Documentation (High, Moderate, Low)	Assurance	P2

Control:

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

Supplemental 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. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, AS-5, CM-2, CP-2; OMB Memo: M-16-04	**Related Controls Requirement(s):** CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.

SA-8	Security Engineering Principles (High, Moderate)	Assurance	P1

Control:

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Implementation Standards:

High & Moderate:

Std.1 - The information system must follow system security engineering principles consistent with:
(a) The information security steps of the CMS eXpedited Life Cycle (XLC) to incorporate information security control considerations;
(b) The information system architecture defined within the Technical Reference Architecture (TRA); and
(c) The Technical Review Board (TRB) processes defined by CMS.

Supplemental Guidance:

Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. 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 on how to build secure software;
(vi) Tailoring security controls to meet organizational and operational needs;
(vii) Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and
(viii) Reducing risk to acceptable levels, thus enabling informed risk management decisions.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

When applying information system security engineering principles in the specification, design, development, implementation, and modification of an information system containing personally identifiable information (PII), the organization should apply privacy-enhanced system design and development principles described in NIST SP 800-53, Rev. 4, Appendix J.

Reference(s): E-Government Act of 2002 (Pub. L. 107-347) §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3; NIST SP: 800-27; OMB Memo: M-16-04, M-05-08, M-03-22; OMB Circular A-130: 7.g.	**Related Controls Requirement(s):** PM-7, SA-3, SA-4, SA-17, SC-2, SC-3, AR-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records.
Interview: Organizational personnel with information system design, development, implementation, and modification responsibilities.

SA-9	External Information System Services (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities regarding external information system services in a SLA or similar agreement; and
c. Employs defined processes, methods, and techniques (defined in the applicable system security plan [SSP]) to monitor security control compliance by external service providers on an ongoing basis.

Implementation Standards:

Systems processing, storing, or transmitting PHI:

PHI.1 - A covered entity or business associate under HIPAA or HITECH may create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations.

Supplemental 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. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the Federal Government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, 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. For services that are 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 provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. 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.

Guidance for systems processing, storing, or transmitting PHI:

The information security requirements and controls are documented through a written contract, or other arrangement that meets the requirements of 45 C.F.R. §164.314(a). This guidance is not intended to cover the acquisition of services of all third-party providers, only those who rise to the level of a business associate of a covered entity.

Reference(s): FedRAMP Rev. 4 Baseline; HIPAA: 45 C.F.R. §164.530; 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.308(b)(4), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii); Homeland Security Presidential Directive (HSPD) 7: D(8); NIST SP: 800-35; OMB Memo: M-16-04;	**Related Controls Requirement(s):** CA-3, IR-7, PS-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PHI:

The organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing external 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; and other relevant documents or records.
Examine: Organization facilitates required oversight of privacy reporting by CMS (to include coordination and cooperation with the CMS Cybersecurity Integration Center [CCIC]).
Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

Systems processing, storing, or transmitting PHI:

Examine: Business associate assurance documentation. (See HIPAA 164.308(b), 164.314(a), and 164.530)
Interview: Organizational personnel responsible for maintaining business associate assurance documentation. (See HIPAA 164.308(b), 164.314(a), and 164.530)

SA-9(2)	Identification of Functions/Ports/Protocols/Services (High, Moderate)	Assurance	P1

Control:

The organization requires providers of external information system services, as defined in the applicable System Security Plan, to identify the functions, ports, protocols, and other services required for the use of such services.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** CM-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing external 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.

SA-9(5)	Non-Mandatory: Processing, Storage, and Service Location	P3

Control:

Systems processing, storing, or transmitting PII (to include PHI):

If the service provider will be maintaining personally identifiable information (PII) outside of the United States, the organization must evaluate the legal environment of the country in which the information will be maintained to ensure US equities are protected. If the service provider is in the US and the PII is about non-US Citizens, then the organization must address the data transfer requirements of the country whose citizens PII is collected or maintained and must ensure that country's privacy/data protection legal requirements are met. The organization must coordinate with its legal counsel, privacy office, and Department of State representative in meeting this requirement.

Systems defined as CSPs:

The organization restricts the location of information processing, information/data, and information system services to organization-defined locations based on program requirements or conditions. In no case may the safeguards afforded to sensitive information be less than the safeguards mandates by CMS, federal law, Executive Order, or other authoritative direction.

Supplemental Guidance:

Guidance for systems processing, storing, or transmitting PII (to include PHI):

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. The criteria external providers use for the selection of processing, storage, or service locations may be 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, 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.
Other countries have different requirements for the protection of PII of either their own citizens or for transfer of PII across national borders. When selecting a service provider, the location for storage, maintenance, or processing must be considered. Some organizations, such as European Union member states, have very stringent data transfer restriction requirements and your organization may have a treaty or other agreement for data exchange and/or protection. Consult with your legal counsel or your organization's liaison to the Department of State.

Reference(s): FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g., 9.b and 9.c.	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing external 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.

SA-10	Developer Configuration Management (High, Moderate)	Assurance	P1

Control:

The organization requires the developer of the information system, system component, or information system service to:
a. Perform configuration management during system, component, or service development, implementation, and operation;

b. Document, manage, and control the integrity of changes to configuration items under configuration management;
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles (defined in the applicable system security plan [SSP]).

Supplemental Guidance:

This control also applies to organizations conducting internal information systems development and integration. 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3; NIST SP: 800-128; OMB Memo: M-16-04	**Related Controls Requirement(s):** CM-3, CM-4, CM-9, SA-12, SI-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records.
Interview: Organization personnel with information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities.

SA-11	Developer Security Testing and Evaluation (High, Moderate)	Assurance	P2

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 CMS procedures;
b. Perform unit; integration; system; and regression testing/evaluation in accordance with the CMS eXpedited Life Cycle (XLC);
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.

Systems processing, storing, or transmitting PII (to include PHI):

For information systems containing PII, the organization requires the developer of the information system, system component, or information system service to:
a. Create and implement a security assessment plan that includes assessment of privacy controls.
b. Conduct tests that:
1. Minimize to the use of PII to the maximum extent practicable;
2. Use actual PII only if a formal memorandum of agreement (MOA), memorandum of understanding (MOU), or data exchange agreement has been established between the data owner of the PII and the entity developing/testing the information system including how loss, theft, or compromise (i.e., breach) of PII is to be handled;
3. Use de-identified or anonymized PII to the maximum extent practicable; and
4. Coordinate use of PII with the privacy office before conducting any testing.

Implementation Standards:

High & Moderate:

Std.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 after the assessment and after selective verification of the results.
Std.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. **Std.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 (ACLs) as well as ports and protocols.

Supplemental 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Testing is a key method to ensure privacy controls are implemented. Including privacy controls in the security assessment plan ensures they are tested.

Reference(s): Code: 5 U.S.C. §552a(e)(10); E-Government Act of 2002 (Pub. L. No. 107-347), §208, and Title III; FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3; ISO/IEC: 15408; OMB Memo: M-03-22; OMB Circular A-130: 7.g.; Web: capec.mitre.org, cve.mitre.org, cwe.mitre.org, nvd.nist.gov	**Related Controls Requirement(s):** CA-2, CM-4, SA-3, SA-4, SA-5, SI-2, AR-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization has implemented all elements of this control as described in the PII control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records.
Interview: Organizational personnel with developer security testing responsibilities.

SA-11(5)	Non-Mandatory: Penetration Testing/Analysis	P3

Control:

The organization requires information systems, system components, and information system services to undergo penetration testing prior to deployment in the production environment, in a manner that is no less stringent than required under CA-8.

Systems processing, storing, or transmitting PII (to include PHI):

If the system contains personally identifiable information (PII), then the penetration testing requirements of CA-8, as specified above in this overlay, must be applied.

Supplemental Guidance:

Penetration testing is an assessment methodology in which assessors, using all available information technology product and/or information system documentation (e.g., product/system design specifications, source code, and administrator/operator manuals) and working under specific constraints, attempt to circumvent implemented security features of information technology products and information systems. Penetration testing can include, for example, white, gray, or black box testing with analyses performed by skilled security professionals simulating adversary actions. The objective of penetration testing is to uncover potential vulnerabilities in information technology products and information systems resulting from implementation errors, configuration faults, or other operational deployment weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Provides for implementation of penetration testing as identified in CA-8.

Reference(s): Code: 5 U.S.C. §552a(b) and (e)(10); NIST SP: 800-115; General Accounting Office (GAO); OMB Circular A-130: 7.g. and 8.b.(2)(c)(iii)	**Related Controls Requirement(s):** CA-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; and other relevant documents or records.
Interview: Organizational personnel with developer security testing responsibilities.
Test: Organizational processes for monitoring developer security testing and evaluation; automated mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation.

SA-11(8)	Non-Mandatory: Dynamic Code Analysis	P3

Control:

The organization requires information systems, system components, and information system services to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance:

Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the way it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).

Reference(s): FedRAMP Rev. 4 Baseline; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; and other relevant documents or records.
Interview: Organizational personnel with developer security testing responsibilities.

SA-12	Supply Chain Protection (High)	Assurance	P1

Control:

The organization protects against supply chain threats to the information system, system component, or information system service by employing best practices and methodologies; and wherever possible, selecting components that have been previously reviewed by other government entities (e.g., National Information Assurance Partnership [NIAP]) as part of a comprehensive, defense-in-breadth information security strategy.

Supplemental Guidance:

Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

Reference(s): NIST IR: 7622; NIST SP: 800-161; OMB Memo: M-16-04	Related Controls Requirement(s): AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts and service level agreements; list of supply chain threats; list of measures to be taken against supply chain threats; information system development life cycle documentation; other relevant documents or records.

SA-15	Development Process, Standards, and Tools (High, Moderate)	Assurance	P2

Control:

The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:

1. Explicitly addresses security requirements;
2. Identifies the standards and tools used in the development process;
3. Documents the specific tool options and tool configurations used in the development process; and
4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Reviews the development process, standards, tools, and tool options/configurations at least every three (3) years to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable System Acquisition (SA) and Configuration Management (CM) security controls.

Supplemental Guidance:

Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.

Reference(s): OMB Memo: M-16-04	Related Controls Requirement(s): SA-3, SA-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records.
Interview: Organizational personnel with developer security testing responsibilities.

SA-15(9)	Use of Live Data (High, Moderate)	P2

Control:

The organization disallows use of live data in development and test environments for the information system, system component, or information system service without prior approval of the Authorizing Official (AO). If approved by the AO, the organization documents and controls the use of live data in the development and test environments for the information system, system component, or information system service at a level commensurate with the sensitivity of the data and way that minimizes the use of live data.

Systems processing, storing, or transmitting PII (to include PHI):

Before use of live data containing personally identifiable information (PII) in a preproduction environment, the organization must:
a. Implement policies and procedures in coordination with the privacy office for evaluating the risk of use of PII in a preproduction environment;
b. Protect, per NIST SP 800-122, the PII within the preproduction environment at the same level as in the production environment; and
c. Use anonymized data substitution (See NIST SP 800-122, Section 4.2.4) if possible.

Supplemental Guidance:

The use of live data in preproduction environments can result in significant risk to organizations. Organizations can minimize such risk by using test or dummy data during the development and testing of information systems, information system components, and information system services.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Preproduction environments may not be as formally controlled as production environments. Use of sensitive information, including PII, in a preproduction environment increases risk to the organization, because the preproduction environment may not be as secure as the production environment.
If PII will be provided to a third-party during testing, the organization will need a formal MOA, MOU, or data exchange agreement before providing access to that third-party. Such agreement will at a minimum include how loss, theft, or compromise of PII is to be handled.

Reference(s): Code: 5 U.S.C. §552a(b) and (e)(10); NIST SP 800-122	**Related Controls Requirement(s):** SA-9, DM-1(1), DM-3, UL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization has implemented all elements of this control as described in the PII control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing development process, standards, and tools; solicitation documentation; acquisition documentation; service-level agreements; acquisition contracts for the information system, system component, or information system service; information system design documentation; information system configuration settings and associated documentation; documentation authorizing use of live data in development and test environments; and other relevant documents or records. **Interview:** Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; system developer. **Test:** Organizational processes for approving, documenting, and controlling the use of live data in development and test environments; automated mechanisms supporting and/or implementing the approval, documentation, and control of the use of live data in development and test environments.

SA-16	Developer-Provided Training (High)	Assurance	P2

Control:

The organization requires the developer of the information system, system component, or information system service to provide appropriate training (or training materials), for affected personnel, on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Supplemental Guidance:

This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training.
Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms.

Reference(s):	**Related Controls Requirement(s):** AT-2, AT-3, SA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records.
Interview: Organizational personnel with developer security testing responsibilities.

SA-17	Developer Security Architecture and Design (High)	Assurance	P1

Control:

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:
a. Is consistent with and supportive of the organization's security architecture (see PL-8), which is established within and is an integrated part of the organization's enterprise architecture (see PM-7);
b. Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and
c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Systems processing, storing, or transmitting PII (to include PHI):

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that accurately and completely describes the privacy requirements and the allocation of security and privacy controls among physical and logical components.

Supplemental Guidance:

This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture, and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities and there is a requirement to demonstrate consistency with the organization's enterprise architecture and information security architecture.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The security architecture and design identifies security and privacy controls necessary to support privacy requirements. The CMS Senior Official for Privacy is the best resource for identifying privacy requirements and privacy controls.

Reference(s): Code: 5 U.S.C. §552a(e)(10); E-Government Act of 2002 (Pub. L. No. 107-347) Title III; OMB Memo: M-05-08	**Related Controls Requirement(s):** PL-8, PM-7, SA-3, SA-8, AR-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records.
Interview: Organizational personnel with developer security testing responsibilities.

SA-22	Non-Mandatory: Unsupported System Components	P3

Control:

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

Supplemental 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.

Reference(s): FISCAM: AS-3, CM-2; HHS: End of Life Operating Systems and Applications Policy; NIST SP: 800-70, 800-128; OMB Memo: M-07-18, M-08-22, M-16-04; Web: checklists.nist.gov, nsa.gov, nvd.nist.gov	**Related Controls Requirement(s):** PL-2, SA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information system, devices, appliances and applications for versions that are no longer supported.
Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel responsible for configuration management.
Test: Automated mechanisms supporting and/or implementing replacement of unsupported system components.

B.16 System and Communications Protection (SC)

SC-1	System and Communications Protection Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates (as necessary) the current:

1. System and communications protection policy within every three (3) years; and

2. System and communications protection procedures within every three (3) years.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; NIST SP: 800-12, 800-100	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy and procedures; system security plan; and other relevant documents or records.
Interview: Organizational personnel with system and communications protection responsibilities. Verify personnel:
1. Know of system and communications protection policy and procedures; and
2. Are responsible for reviewing and updating system and communications protection policy and procedures no less often than required.

SC-2	Application Partitioning (High, Moderate)	Assurance	P1

Control:

The information system separates user functionality (including user interface services) from information system management functionality.

Systems processing, storing, or transmitting PII (to include PHI):

In any situation where personally identifiable information (PII) is present, PII must be stored on a logical or physical partition separate from the applications and software partition.

Supplemental Guidance:

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, and servers and typically requires privileged user access. The separation of 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

It is necessary to store sensitive information, such as PII, on separate logical partitions from applications and software that provide user functionality to restrict accidental or unintentional loss of, or access to, sensitive information by both unauthorized users and unauthorized applications.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-4, AS-2; 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g. and 8.b.(3); 45 C.F.R. §164.312(a)(1)	**Related Controls Requirement(s):** SA-4, SA-8, SC-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

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; other relevant documents or records.
Test: Separation of user functionality from information system management functionality.

Systems processing, storing, or transmitting PII (to include PHI):

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system separate user functionality (including user interface services) from information system management functionality.
Test: Separation of user functionality from information system management functionality.

SC-3	Security Function Isolation (High)	Assurance	P1

Control:

The information system isolates security functions from non-security functions.

Supplemental Guidance:

The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems implement code separation (i.e., separation of security functions from non-security functions) in several ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code. Information systems restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include non-security functions within the isolation boundary as an exception.

Reference(s): FISCAM: AC-4, AS-2	**Related Controls Requirement(s):** AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from non-security functions; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information systems separate the security functions of the information system from non-security functions.
Test: Separation of security functions from non-security functions within the information system.

SC-3(2)	Non-Mandatory: Access/Flow Control Functions	Assurance	P3

Control:

The information system isolates security functions enforcing access and information flow control from non-security functions and from other security functions.

Supplemental Guidance:

Security function isolation occurs because of implementation; the functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include, for example, auditing, intrusion detection, and anti-virus functions.

Reference(s): NIST SP: 800-160	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing security function isolation; list of critical security functions; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information systems provide the capability to enforce access and flow controls separating security functions and non-security functions.
Test: Isolation of security functions enforcing access and information flow control.

SC-3(3)	Non-Mandatory: Minimize non-security Functionality	Assurance	P3

Control:

The organization minimizes the number of non-security functions included within the isolation boundary containing security functions.

Supplemental Guidance:

Where it is not feasible to achieve strict isolation of non-security functions from security functions, it is necessary to take actions to minimize the non-security-relevant functions within the security function boundary. Non-security functions contained within the isolation boundary are considered security-relevant because errors or maliciousness in such software, by being within the boundary, can impact the security functions of organizational information systems. The design objective is that the specific portions of information systems providing information security are of minimal size/complexity. Minimizing the number of non-security functions in the security-relevant components of information systems allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing non-security functions within the isolation boundaries, the amount of code that must be trusted to enforce security policies is reduced, thus contributing to understandability.

Reference(s): NIST SP: 800-160	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-4	Information in Shared Resources (High, Moderate)	P1

Control:

The information system prevents unauthorized and unintended information transfer via shared system resources.

Implementation Standards:

High & Moderate:

Std.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. 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.

Supplemental 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Following use of a shared system resource, ensure that shared system resource(s) is purged of personally identifiable information (PII) to prevent unintended users or processes from accessing PII.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-4, AS-2; 5 U.S.C. §552a(b) and (e)(10); OMB Circular A- 130, 7.g. and 8.b.(3); 45 C.F.R. §164.312(a)(1)	**Related Controls Requirement(s):** AC-3, AC-4, MP-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The information system prevents unauthorized and unintended information transfer via shared system resources; and
(ii) The organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing information remnants; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system for unauthorized and unintended transfer of information via shared system resources.

Systems processing, storing, or transmitting PII (to include PHI):

Examine: System and communications protection policy; procedures addressing information remnants; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system implement functionality that prevents unauthorized and unintended information transfers via shared system resources.
Test: Information system for unauthorized and unintended transfer of information via shared system resources.

SC-5	Denial of Service Protection (High, Moderate, Low)	P1

Control:

The information system protects against or limits the effects of the types of denial of service attacks defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable system security plan):
- SANS Organization: www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating Distributed Denial of Service (DDoS): www.sans.org/dosstep/roadmap.php; and
- NIST National Vulnerability Database: http://nvd.nist.gov/home.cfm.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, 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. The list of denial of service attack types is approved and accepted by the Joint Authorization Board (JAB).

Low:

CSP.1 - For CSPs, 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. The list of denial of service attack types is approved and accepted by the JAB).

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2	**Related Controls Requirement(s):** SC-6, SC-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system for protection against or limitation of the effects of denial of service attacks.

SC-7	Boundary Protection (High, Moderate, Low)	P1

Control:

The information system:
a. Monitors and controls communications at the external boundary, both physically and logically, of the system and at key internal boundaries within the system;
b. Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
Std.2 - Utilize stateful inspection/application firewall hardware and software.
Std.3 - Utilize firewalls from two (2) or more different vendors at the various levels within the network to reduce the possibility of compromising the entire network. **Std.4 -** If the system has an outward facing Web or email presence to the public internet, the organization must implement and support a technical capability to detect malware in web traffic traversing the organization's boundary by:
(a) Monitoring assets without the need to deploy software agents (zero client footprint);
(b) Dynamically generating actionable malware intelligence;
(c) Detecting and stopping web-based and email attacks; and
(d) Sending alert data to the organization's SIEM.
Std.5 - Aggregated boundary protection device information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include boundary protection systems, appliances, devices, services, and applications; and
(c) CCIC directed aggregated boundary protection device information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.6 - As required by CMS, raw boundary protection device information from relevant automated must be available in an unaltered format to the CCIC.

Supplemental 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 (DMZ). 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 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.
Contact your CRA or the CCIC for the list of compliant formats.

Reference(s): FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-1, AS-2; NIST SP: 800-41, 800-77, 800-137; 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(i)	**Related Controls Requirement(s):** AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; and other relevant documents or records.
Examine: Information systems documentation describing boundary protection mechanisms at external connections, between zones, and at the host level.
Interview: Selected organizational personnel with boundary protection responsibilities.
Test: Mechanisms implementing boundary protection capability within the information system.

SC-7(3)	Access Points (High, Moderate)	P1

Control:

The organization limits the number of external network connections to the information system.

Implementation Standards:

High & Moderate:

Std.1 - Implementation must route external connections via a Trusted Internet Connection (TIC) portal.

Systems defined as CSPs:

High & Moderate:

CSP.1 - Implementation must be compliant with FedRAMP interconnection requirements.

Supplemental Guidance:

Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The TIC initiative is an example of limiting the number of external network connections.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.

SC-7(4)	External Telecommunications Services (High, Moderate)	P1

Control:

The organization:
(a) Implements a managed interface for each external telecommunication service;
(b) Establishes a traffic flow policy for each managed interface;
(c) Protects the confidentiality and integrity of the information being transmitted across each interface;
(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
(e) Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days or implementation of major new system, and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** SC-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing boundary protection; traffic flow policy; 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; and other relevant documents or records.
Interview: Selected organizational personnel with boundary protection responsibilities.

SC-7(5)	Deny by Default/Allow by Exception (High, Moderate)	P1

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).

Supplemental 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 which are essential and approved are allowed.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Interview: Selected organizational personnel with boundary protection responsibilities.

SC-7(7)	Prevent Split Tunneling for Remote Devices (High, Moderate)	P1

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.

Supplemental 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 VPN for remote connections, when 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 to prevent split tunneling.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Automated mechanisms supporting non-remote connections with the information system.

SC-7(8)	Route Traffic to Authenticated Proxy Servers (High)	P1

Control:

The information system routes all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, this Standard replaces the requirement defined in SC-07(08). 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.
CSP.2 - For CSPs, 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. The internal communications traffic and external networks are approved and accepted by Joint Authorization Board (JAB).

Supplemental 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 TCP sessions and blocking specific URLs, domain names, and IP addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AC-3, AU-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Mechanisms implementing managed interfaces within information system boundary protection devices.

SC-7(18)	Fail Secure (High)	Assurance	P1

Control:

The information system fails securely in the event of an operational failure of a boundary protection device.

Supplemental 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 unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** CP-2, SC-24

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.

SC-7(21)	Isolation of Information System Components (High)	Assurance	P1

Control:

The organization employs boundary protection mechanisms to separate defined information system components (defined in the applicable system security plan) supporting CMS missions and/or business functions.

Supplemental Guidance:

Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber-attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls; separating system components into physically separate networks or subnetworks; cross-domain devices separating subnetworks; virtualization techniques; and encrypting information flows among system components using distinct encryption keys.

Reference(s):	**Related Controls Requirement(s):** CA-9, SC-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.

SC-8	Transmission Confidentiality and Integrity (High, Moderate)	P1

Control:

The information system protects the confidentiality and integrity of information. Any transmitted data containing sensitive information must be encrypted using a FIPS 140-2 validated module (See SC-13 and *HHS Standard for Encryption of Computing Devices and Information*).

Supplemental 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, 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 physical 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 which 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Because of the sensitivity of personally identifiable information (PII) and protected health information (PHI), the confidentiality and integrity of such information in transit must be assured.

Reference(s): FedRAMP Rev. 4 Baseline; Code: 5 U.S.C. §552a(e)(5) and (10); E-Government Act of 2002 (I; Pub. L. No. 107-347), Title III; FIPS Pub: 140-2, 197; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(c)(2), 45 C.F.R. §164.312(e)(2)(i); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(e)(1); HHS: IS2P 2014; NIST SP: 800-52, 800-77, 800-81, 800-113; OMB Circular A-130: 7.g. and Appendix 1	**Related Controls Requirement(s):** AC-17, PE-4, SI-04, AR-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information systems and devices restrict the use of unapproved transmission protocols (including wireless protocols).
Test: Transmission integrity capability within the information system.

SC-8(1) Cryptographic or Alternate Physical Protection (High, Moderate) P1

Control:

The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by approved alternative safeguards and defined in the applicable system security plan and Information System Risk Assessment.

Systems processing, storing, or transmitting PII (to include PHI):

FIPS-validated encryption or protected distribution systems are used to protect personally identifiable information (PII) to ensure the information's confidentiality and integrity during transmission.

Supplemental 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 which have common application in digital signatures, checksums, and message authentication codes. However, protected distribution systems can achieve similar results while allowing continuous monitoring of traffic and content through automated DLP systems.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Because of the sensitivity of PII, the confidentiality and integrity of such information in transit must be assured with encryption techniques if assurance is not provided by other means.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

Reference(s): Code: 5 U.S.C. §552a(e)(5) and (10); E-Government Act of 2002 (Pub. L. No. 107-347), Title III; FedRAMP Rev. 4 Baseline; OMB Memo: M-17-12 Att. 1, C., M-06-16; OMB Circular A-130: 7.g. and Appendix 1; 45 C.F.R. §164.312(c)(2); 45 C.F.R.§164.312(e)(2)(i)	**Related Controls Requirement(s):** SC-13

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Cryptographic mechanisms implementing transmission integrity capability within the information system.

SC-8(2)	Non-Mandatory: Pre/Post Transmission Handling	P3

Control:

The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Because of the sensitivity of personally identifiable information (PII), the integrity of information in transit must be assured at all points during aggregation, packaging and transformation.

Reference(s): 5 U.S.C. §552a(e)(5) and (10); OMB Memo: M-17-12, Att. 1, C., M-06-16; OMB Circular A-130: 7.g. and 8.b.(3) and Appendix 1	**Related Controls Requirement(s):** AC-13, AU-10

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Transmission integrity capability within the information system.

SC-10	Network Disconnect (High, Moderate)	P2

Control:

The information system:
a. terminates the network connection associated with a communications session at the end of the session, or:
1. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and
2. Forcibly disconnects inactive VPN connections after thirty (30) minutes or less of inactivity; and
b. terminates or suspends network connections (i.e., a system to system interconnection) upon issuance of an order by the CMS CIO, CISO, or Senior Official for Privacy (SOP).

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, this Standard replaces the requirement defined within SC-10. The information system terminates the network connection associated with a communications session at the end of the session, or after thirty (30) minutes for all RAS-based sessions and thirty (30) to sixty (60) minutes for non-interactive users, of inactivity.
CSP.2 - For CSPs, long running batch jobs and other operations are not subject to this time limit.

Supplemental 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, 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B); NIST SP: 800-40, 800-47, 800-182	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined period of inactivity before network disconnect; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system functionality include an idle process disconnection capability.
Examine: Information system functionality includes the ability to terminate or suspend communications on a system interconnection.
Test: Network disconnect capability within the information system.

SC-12	Cryptographic Key Establishment and Management (High, Moderate, Low)	P1

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 the *HHS Standard for Encryption of Computing Device* and organizationally-defined requirements (defined in, or referenced by, the applicable System Security Plan) for key generation, distribution, storage, access, and destruction.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Because cryptography is desired to protect sensitive information such as personally identifiable information (PII) and protected health information (PHI), cryptographic key establishment and management must be performed in such a way that even the loss of keys will not permit access to the sensitive information.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

Reference(s):	**Related Controls Requirement(s):** SC-13, SC-17

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel with responsibilities for cryptographic key establishment or management.
Test: Automated mechanisms implementing cryptographic key management and establishment within the information system.

SC-12(1)	Availability (High)	P1

Control:

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Implementation Standards:

High:

Std.1 - Mechanisms are employed to:
(a) Prohibit the use of encryption keys that are not recoverable by authorized personnel;
(b) Require senior management approval to authorize recovery of keys by other than the key owner; and
(c) Comply with approved cryptography standards (see SC-13).

Supplemental Guidance:

Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.

SC-13	Cryptographic Protection (High, Moderate, Low)	P1

Control:

The information system implements cryptographic mechanisms, in transit and at rest, as defined in the HHS Standard for Encryption of Computing Devices and Information, and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental 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 (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).
This control applies to applications with an integrated access control mechanism, such as WinZip and SecureZip, as well as the underlying operating system. These applications must meet CMS (FIPS 140-2 validated module) requirements.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

FIPS-validated cryptographic modules are the government standard for encryption. When sensitive information such as PII requires encryption, the organization must comply with these standards.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.

SC-15	Collaborative Computing Devices (High, Moderate, Low)	P1

Control:

The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If collaborative computer is authorized, the authorization must specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. 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.

Implementation Standards:

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the information system prohibits remote activation of collaborative computing devices with no exceptions.
CSP.2 - For CSPs, the information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

Supplemental Guidance:

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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2	**Related Controls Requirement(s):** AC-21

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users.

SC-15(1)	Physical Disconnect (High, Moderate, Low)	P1

Control:

If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

Supplemental Guidance:

Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants carry out the disconnection activity without having to go through complex and tedious procedures.

Reference(s): NIST SP: 800-47, CMS CIO Directive 14-03	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information systems implements functionality that provides an override of interconnections in manner that supports ease of use.
Test: Physical disconnect of collaborative computing devices.

SC-17	Public Key Infrastructure Certificates (High, Moderate)	P1

Control:

The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the Joint Authorization Board (JAB).

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-32, 800-63; OMB Memo: M-05-24	**Related Controls Requirement(s):** SC-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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.
Interview: Organizational personnel with public key infrastructure certificate issuing responsibilities.

SC-18	Mobile Code (High, Moderate)	P2

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.

Supplemental 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., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-4, AS-2; NIST SP: 800-28	**Related Controls Requirement(s):** AU-2, AU-12, CM-2, CM-6, SI-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Interview: Organizational personnel with mobile code authorization, monitoring, and control responsibilities.
Test: Mobile code authorization and monitoring capability for the organization.

SC-19	Voice Over Internet Protocol (High, Moderate)	P1

Control:

The organization prohibits the use of VoIP technologies, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If VoIP is authorized, the organization:
a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously;
b. Authorizes, monitors, and controls the use of VoIP within the information system; and
c. Ensures VoIP equipment used to transmit or discuss sensitive information is protected with CMS (FIPS 140-2 validated module) encryption requirements.

Supplemental Guidance:

VoIP applications and devices must be configured meet CMS (FIPS 140-2 validated module) requirements.
FIPS 140-2 approved security function families are found at http://csrc.nist.gov/groups/STM/cavp/validation.html. However, implementing an approved security function is the start. The product must also be on the approved validation lists. (See http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm for a list of current validated products.)

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; NIST SP: 800-58	**Related Controls Requirement(s):** CM-6, SC-7, SC-15

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; other relevant documents or records.
Interview: Organizational personnel with VoIP authorization and monitoring responsibilities.
Test: VoIP authorization and monitoring capability for the organization.

SC-20	Secure Name/Address Resolution Service (Authoritative Source) (High, Moderate, Low)	P1

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.

Supplemental 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 service (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 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-81; OMB Memo: M-08-23	Related Controls Requirement(s): AU-10, SC-8, SC-12, SC- 13, SC-21, SC-22

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information system implements secure resolution services. Examples:
1. DNSSEC
2. Name resolution is configured to maximize security (e.g., disallow recursive lookups as appropriate)
Test: Automated mechanisms implementing secure name/address resolution service (authoritative source).

SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) (High, Moderate, Low) P1

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.

Supplemental 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 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-81	Related Controls Requirement(s): SC-20, SC-22

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms implementing data origin authentication and integrity verification for resolution services.

SC-22 Architecture and Provisioning for Name/Address Resolution Service (High, Moderate, Low) P1

Control:

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental 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 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-81	**Related Controls Requirement(s):** SC-2, SC-20, SC-21, SC-24

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Automated mechanisms supporting name/address resolution service for fault tolerance and role separation.

SC-23	Session Authenticity (High, Moderate)	P1

Control:

The information system protects the authenticity of communications sessions.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-52, 800-77, 800-95	**Related Controls Requirement(s):** SC-8, SC-10, SC-11

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Automated mechanisms implementing session authenticity.

SC-24	Fail in Known State (High)	Assurance	P1

Control:

The information system fails to a known secure state for all failures preserving the maximum amount of state information in failure.

Supplemental Guidance:

Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.

Reference(s):	**Related Controls Requirement(s):** CP-2, CP-10, CP-12, SC- 7, SC-22

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; procedures addressing information system failure; information system design documentation; information system configuration settings and associated documentation; list of failures requiring information system to fail in a known state; state information to be preserved in system failure; other relevant documents or records.
Test: Automated mechanisms implementing fail-in-known-state capability.

SC-28 | Protection of Information at Rest (High, Moderate) | P1

Control:

The information system protects the confidentiality and integrity of information at rest, as defined in the *HHS Standard for Encryption of Computing Devices and Information*.

Systems processing, storing, or transmitting PII (to include PHI):

The information system protects the confidentiality and integrity of personally identifiable information (PII).

Systems defined as CSPs:

For CSPs, the information system enforces encryption of the instance (container) image files under the hypervisor:
- Instance (container) image files from virtual server and client deployments must be encrypted in a manner that meets FIPS 140-2 validated requirements.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs support the capability to use cryptographic mechanisms to protect information at rest.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Because of the sensitivity of PII and protected health information (PHI), the confidentiality and integrity of such information must be assured for data at rest.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-56, 800-57, 800-111; 5 U.S.C. §552a(b) and (e)(10); OMB Memo: M-06-16, M-17-12 Att. 1, C.; 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R.§164.312(e)(2)(ii)	**Related Controls Requirement(s):** AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

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; and other relevant documents or records.
Test: Automated mechanisms implementing confidentiality and integrity protections for information at-rest.

SC-28(1) | Non-Mandatory: Cryptographic Protection | P3

Control:

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of CMS Sensitive Information as defined in the Risk Management Handbook (RMH), *Volume 1, Chapter 10, CMS Risk Management Terms, Definitions, and Acronyms*.

Systems processing, storing, or transmitting PII (to include PHI):

Organizations must:
1. Encrypt data at rest in mobile devices for confidentiality to protect against loss, theft, or compromise;
2. Encrypt data stored in network share drives to insure confidentiality;
3. Encrypt storage/back-up data where physical protection is either not available, not implemented, or not audited;
4. If assurance is not provided by other means, encrypt personally identifiable information (PII) in a database; and
5. Encrypt data stored in the cloud—whether the cloud is government or private.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - CSPs support the capability to use cryptographic mechanisms to protect information at rest.

Supplemental Guidance:

Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.
For additional Guidance, see: HHS Standard for Encryption of Computing Devices and Information.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Because of the sensitivity of PII and PHI, the confidentiality and integrity of such information must be assured for data at rest using encryption technologies if assurance is not provided by other means.
Organizations may use file share scanning (e.g., data loss prevention [DLP] technology) to ensure compliance with the requirement to encrypt PII/protected health information (PHI) at rest.

Guidance for systems processing, storing, or transmitting PHI:

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized.

Reference(s): Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16, M-17-12 Att. 1, C., 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R.§164.312(e)(2)(ii)	**Related Controls Requirement(s):** AC-13, AC-19, SC-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Test: Automated mechanisms implementing confidentiality and integrity protections for information at-rest.

SC-39	Process Isolation (High, Moderate, Low)	Assurance	P1

Control:

The information system maintains a separate execution domain for each executing process.

Supplemental 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 so that communication between processes is performed in a manner controlled through the security functions, 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and communications protection policy; 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; other relevant documents or records.
Interview: Organizational personnel installing, configuring, and/or maintaining the information system.

SC-CMS-1	Electronic Mail (High, Moderate)	P2

Control:

Controls must be implemented to protect sensitive information that is sent via email.

Implementation Standards:

High & Moderate:

Std.1 - Email and any attachment that contains sensitive information when transmitted inside and outside of HHS premises shall be encrypted using the user's Personal Identity Verification (PIV) card when possible. If PIV encryption is not feasible, a FIPS 140-2 validated solution must be employed:
- Password protection of files is recommended to add an additional layer of data protection but shall not be used in lieu of encryption solutions.
- Password and/or encryption key shall not be included in the same email that contains sensitive information or in separate email. Password/encryption key shall be provided to the recipient separately via text message, verbally, or other out-of-band solution.

Std.2 - MFA is required before being granted access to CMS email.
Std.3 - MFA access control mechanisms must meet CMS approved standards discussed in the RMH, *Volume III, Standard 3.1, CMS Authentication Standards*.

Supplemental Guidance:

This control acknowledges the sensitive nature of much of the information CMS handles, especially within email. For guidance and recommended security practices for handling sensitive information via email see NIST SP 800-45 (as amended), Guidelines on Electronic Mail Security.

Reference(s): HSPD: HSPD-12; NIST SP: 800-45	**Related Controls Requirement(s):** SI-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Email policy and procedures; and other relevant documents or records.

Examine: Information system enforces approved multifactor authentication for access to email.
Interview: Sample of organizational personnel who use email.

SC-CMS-2	Website Usage (High, Moderate, Low)	P2

Control:

Websites are operated within the restrictions addressed in OMB directives M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*, and applicable CMS and HHS directives and instruction.

Implementation Standards:

High & Moderate:

Std.1 - All publicly accessible federal websites and web services shall employ secure connections, such as Hypertext Transfer Protocol Secure (HTTPS).
Std.2 - TLS shall be implemented and configured in accordance with the recommendation of NIST SP 800-52, as amended.
Std.3 - Websites and services shall deploy HTTPS in a manner that allows for rapid updates to certificates, cipher choices protocol versions, and other configuration elements.
Std.4 - Websites and services available over HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS going forward. **Std.5 -** Allowing HTTP connections for the sole purpose of redirecting clients to HTTPS connections shall be acceptable and encouraged. HSTS headers must specify a max-age of at least 1 year.

Supplemental Guidance:

This control monitors the CMS and HHS security programs associated with websites to determine if there are any modified directives and instruction.

Reference(s): OMB Memo: M-10-22, M-10-23, M-15-13	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: CMS website baseline configuration and change management documentation for appropriate configurations.
Interview: Web site administrators.

B.17 System and Information Integrity (SI)

SI-1	System and Information Integrity Policy and Procedures (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates (as necessary) the current:
1. System and information integrity policy at least every three (3) years; and
2. System and information integrity procedures at least every three (3) years.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI 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 information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Policies that support protecting the integrity of systems and information are necessary to meet the Privacy Act requirements to protect against any anticipated threats or hazards to the security or integrity of records.

Reference(s): Code: 5 U.S.C. §552a(b)and (e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R.§164.308(a)(6)(ii); NIST SP: 800-12, 800-100; OMB Memo: M-17-12	**Related Controls Requirement(s):** PM-9

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and information integrity responsibilities.

SI-2	Flaw Remediation (High, Moderate, Low)	P1

Control:

The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates as directed in Implementation Standard 1; and
d. Incorporates flaw remediation into the organizational configuration management process.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Correct identified security-related information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes; and
(b) Manage the flaw remediation process centrally.
Std.2 - A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO or his/her designated representative (e.g., the system data owner or CMS CISO) and updated documentation in the risk analysis and security plan if a security patch is not to be applied to an information technology component or a legacy (no-longer maintained by the vendor) component is to remain in use.
Std.3 - Flaw remediation requirements apply to all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE - identified vulnerability.
Std.4 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational flaw (e.g., patch) status and posture information.

Supplemental 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, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow United States Computer Emergency Readiness Team (US-CERT) guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors, including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). 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 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 are not necessary or practical. Organizations may also consider in testing decisions, whether security- relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.
Operating systems and installed applications, including databases and services, need to be examined.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B); NIST SP: 800-40, 800-37, 800-39, 800-137, 800-182; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):** CA-2, CA-7, CM-3, CM-5, CM-8, IR-4, MA-2, RA-5, SA-10, SA-11, SI-11

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information systems are patched within defined time-frame requirements and patch logs show system is being maintained within required time-frames.
Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(1)	Central Management (High)	P1

Control:

The organization centrally manages the flaw remediation process.

Implementation Standards:

High:

Std.1 - Automated flaw remediation results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Flaw remediation results sources include all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE- identified vulnerability; and
(c) CCIC directed flaw remediation information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - Raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Moderate, & Low:

Std.1 – When selected, automated flaw remediation results must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Flaw remediation results sources include all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE- identified vulnerability; and
(c) CCIC directed flaw remediation information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - When selected, raw security information/results from relevant automated tools must be available in an unaltered format to the CCIC.

Supplemental 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, centrally managed flaw remediation security controls.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information systems demonstrate automated mechanisms are used to remediate flaws.
Test: Mechanisms supporting centralized management of flaw remediation and automatic software updates.

SI-2(2)	Automated Flaw Remediation Status (High, Moderate)	P1

Control:

The organization employs automated mechanisms no less often than once every seventy-two (72) hours to determine the state of information system components regarding flaw remediation.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M- 16-04	**Related Controls Requirement(s):** CM-6, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting 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; and other relevant documents or records.
Examine: Information systems include capability to evaluate flaw remediation within the stated period.
Test: Automated mechanisms implementing information system flaw remediation update status.

SI-3	Malicious Code Protection (High, Moderate, Low)	P1

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 CMS configuration management policy and procedures; and
c. Configures malicious code protection mechanisms to:
1. Perform periodic scans of the information system using the frequency specified in Implementation Standard 1 and Implementation Standard 2, and real-time scans of files from external sources at endpoint, and/or network entry/exit points, as the files are downloaded, opened, or executed in accordance with organizational security policy; and
2. Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Implementation Standards:

High, Moderate, & Low:

Std.1 - Desktop malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.
Std.2 - Server (to include databases and applications) malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.
Std.3 - Malicious code scanning results are reported to the CCIC SIEM in compliance with AU-06.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization configures malicious code protection mechanisms to:
- Perform periodic scans of the information system at least weekly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- Block or quarantine malicious code, send alert to administrator, send alert to FedRAMP in response to malicious code detection.

Supplemental 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, 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.

Guidance for systems processing, storing, or transmitting PHI:

Malicious code protections are essential in system with PHI because of the sensitivity and desirability of such information.

Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; NIST SP: 800-37, 800-39, 800-83, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R. §164.308(a)(6)(ii)	**Related Controls Requirement(s):** CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information systems, databases, and applications employ malicious code protection mechanisms.
Examine: Information systems, databases, and applications employ periodic scans for malicious code.
Interview: Organizational personnel with malicious code protection responsibilities.
Test: Automated mechanisms implementing malicious code protection capability.

SI-3(1)	Central Management (High, Moderate)	P1

Control:

The organization centrally manages malicious code protection mechanisms.

Supplemental 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, centrally managed flaw, malicious code protection security controls.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AU-2, SI-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing malicious code protection; 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.

SI-3(2)	Automatic Updates (High, Moderate)	P1

Control:

The information system automatically updates malicious code protection mechanisms.

Supplemental Guidance:

Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** SI-8

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing malicious code protection; 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.

SI-4	Information System Monitoring (High, Moderate, Low)	Assurance	P1

Control:

The organization:

a. Monitors the information system to detect:
1. Attacks and indicators of potential attacks in accordance with the current RMH, *Chapter 08: Incident Response*; and
2. Unauthorized local, network, and remote connections as defined by (twice High and Moderate or once for Low) weekly;
b. Identifies unauthorized use of the information system through defined techniques and methods (defined in the applicable System Security Plan);
c. Deploys monitoring devices:
1. Strategically within the information system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization.
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion about information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides defined information system monitoring information (defined in the applicable System Security Plan) to defined personnel or roles (defined in the applicable System Security Plan) as needed, and at defined frequency (defined in the applicable System Security Plan).

Implementation Standards:

High, Moderate, & Low:

Std.1 - Implement a centrally managed Intrusion detection system/intrusion protection system (IDS/IPS) capability to monitor network communications on all networks and subnets of any environment requiring a CMS Authority to Operate.
a. Permitted IDS/IPS mechanisms:
- centrally managed IDS/IPS devices at network perimeter points, to include between zones; and
- centrally managed host-based IDS/IPS sensor agents in information technology components for which such agents are available.
b. Environments where communications within the zone are encrypted must use mechanisms capable of either decrypting content for analysis or analyzing content before transmission/after receipt; and
c. Information technology components that do not support host-based IDS/IPS sensors capability must be documented in the applicable risk assessment and security plan.
Std.2 - Monitoring functionality supports the sharing of threat awareness information in a format that meets CMS requirements.
Std.3 - The organization monitors for unauthorized remote connections to the information system continuously, in real-time and takes appropriate action if an unauthorized connection is discovered.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization monitors events on the information system to ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examines system records to confirm that the system is functioning in an optimal, resilient, and secure state; identifies irregularities or anomalies that are indicators of a system malfunction or compromise; and detects information system attacks.

Supplemental 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, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from DHS can also be included as monitoring devices. 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Intrusion-monitoring tools may collect personally identifiable information (PII) of all types. Notice to users who are monitored should be provided prior to system use. Controls sufficient to protect the type of PII collected must be in place for the technology performing the monitoring, including encryption of monitoring data that may contain PII. When conducting information system monitoring on internal or external networks which may collect PII, the organization should coordinate with the organization's counsel and privacy officer.

Reference(s): Code: 5 U.S.C. §552a(b), (e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(5)(ii)(B), 45 C.F.R. §164.308(a)(6)(ii); NIST SP: 800-61, 800-83, 800-92, 800-94, 800-137; OMB Memo: M-17-12, M-14-03, M-15-01, M-16-04; OMB Circular A-130: 7.g.	**Related Controls 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, SC-26, SC-35, SI-3, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that supports monitoring to detect attacks and indicators of potential attacks.
Interview: Organizational personnel with information system monitoring responsibilities.
Test: Automated mechanisms supporting and/or implementing information system monitoring capability.

SI-4(2)	Automated Tools for Real-Time Analysis (High, Moderate)	Assurance	P1

Control:

The organization employs automated tools to support near real-time analysis of events.

Implementation Standards:

High & Moderate:

Std.1 - Aggregated real-time analysis of events information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include events/notifications emanating from local analysis tools and directly from any information technology component in an environment requiring a CMS Authority to Operate; and
(c) CCIC directed real-time analysis of events information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.

Supplemental 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.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-137; OMB Memo: M-14-03, M-15-01	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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 documentation; and other relevant documents or records.
Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that supports near real-time analysis of events.
Test: Automated tools supporting near real-time event analysis.

SI-4(4)	Inbound and Outbound Communications Traffic (High, Moderate)	Assurance	P1

Control:

The information system monitors inbound and outbound communications traffic at a defined frequency (defined in the applicable System Security Plan) for unusual or unauthorized activities or conditions.

Implementation Standards:

High & Moderate:

Std.1 - Aggregated inbound and outbound communications traffic information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include traffic analysis information from local analysis tools and directly from any information technology component in an environment requiring a CMS Authority to Operate; and
(c) CCIC directed aggregated inbound and outbound communications traffic information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.

Supplemental Guidance:

Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-137; OMB Memo: M-14-03, M-15-01	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that supports monitoring of inbound and outbound communications traffic at a defined frequency.
Test: Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms.

SI-4(5)	System-Generated Alerts (High, Moderate)	Assurance	P1

Control:

The information system alerts defined personnel or roles (defined in the applicable System Security Plan) when the following indications of compromise or potential compromise occur:
a. Presence of malicious code;
b. Unauthorized export of information;
c. Signaling to an external information system; or
d. Potential intrusions

Implementation Standards:

High & Moderate:

Std.1 - Aggregated alert information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include all alert-generating information technology components in an environment requiring a CMS Authority to Operate; and
(c) CCIC directed aggregated alert information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw event information must be available in an unaltered format to the CCIC.

Low:

Std.1 – When selected, aggregated alert information must be searchable by the CCIC:
(a) Information is provided to the CCIC in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Information sources include all alert-generating information technology components in an environment requiring a CMS Authority to Operate.
Std.2 - When selected, as required by CMS, raw event information must be available in an unaltered format to the CCIC.

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, this Standard replaces the requirement defined within SI-04(05). The indications that a compromise or potential compromise occurred include: protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline configuration/system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.
CSP.2 - For CSPs, the organization defines additional compromise indicators as needed.

Supplemental 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.
Contact your CRA or the CCIC for the list of compliant formats. All security information and results, complete and unedited, from relevant automated tools must be available to the CCIC upon their request. The information must be made available in a format, and within a timeframe, to be agreed-upon with the CCIC and consistent with all other safeguards required by the ARS.

Guidance for systems defined as CSPs:

Alerts may be generated from a variety of sources, including but not limited to malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

Reference(s): FedRAMP Rev. 4 Baseline; NIST SP: 800-137; OMB Memo: M-14-03, M-15-01	**Related Controls Requirement(s):** AU-5, PE-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; system security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that provides alerts to defined personnel or roles (defined in the applicable System Security Plan) when any of the organization-defined list of compromise or potential compromise indicators occur.
Test: Information system monitoring real-time alert capability.

SI-4(14)	Non-Mandatory: Wireless Intrusion Detection	P3

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.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; GAO finding	**Related Controls Requirement(s):** AC-18, IA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; and other relevant documents or records.
Examine: Organization employs wireless intrusion detection functionality (as systems, devices, appliances or applications) that supports identification of rogue wireless devices.
Interview: Organizational personnel with information system monitoring responsibilities.
Test: Wireless intrusion detection mechanisms.

SI-5	Security Alerts, Advisories, and Directives (High, Moderate, Low)	Assurance	P1

Control:

The organization:
a. Receives information system security alerts, advisories, and directives from defined external organizations (including US-CERT and organizations as defined in the applicable System Security Plan) on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: defined personnel or roles (defined in the applicable System Security Plan); and
d. Implements security directives in accordance with established time frames or notifies CMS of the degree of noncompliance.

Implementation Standards:

High, Moderate, & Low:

Std.1 - The organization's security operations center is responsible for responding to advisories, requests, or directives issued by the CMS Security Operations Center (SOC) and/or CCIC.

Systems defined as CSPs:

High, Moderate, & Low:

CSP.1 - For CSPs, the organization disseminates security alerts, advisories, and directives to all staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP.
CSP.2 - For CSPs, the organization defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives. The list also includes designated FedRAMP personnel.

Supplemental Guidance:

The US-CERT generates security alerts and advisories to maintain situational awareness across the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

Guidance for systems processing, storing, or transmitting PHI:

Receiving and acting on security alerts from US-CERT, or other appropriate organizations, assists in protecting PHI by protecting information systems against rapidly evolving threats. Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s):	**Related Controls Requirement(s):** SI-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Systems defined as CSPs:

(i) The CSP meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; and 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.

SI-5(1)	Automated Alerts and Advisories (High)	Assurance	P1

Control:

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

Supplemental Guidance:

The significant number of changes to organizational information systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk, including the governance level, mission/business process/enterprise architecture level, and the information system level.

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records.
Test: Automated mechanisms implementing the distribution of security alert and advisory information.

SI-6	Security Function Verification (High)	Assurance	P1

Control:

The information system:
a. Verifies the correct operation of defined security functions (defined in the applicable System Security Plan);
b. Performs this verification upon system startup, restart, and upon command by a user with appropriate privileges no less often than once per month;
c. Notifies the system administrators of failed security verification tests; and
d. Shuts the information system down, or restarts the information system, or performs some other defined alternative action(s) (defined in the applicable System Security Plan) when anomalies are discovered.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the information system verifies the correct operation of security functions upon system startup and/or restart and periodically every thirty (30) days and notifies system administrator and performs FedRAMP and CMS-defined actions when anomalies are discovered.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2	**Related Controls Requirement(s):** CA-7, CM-6

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Security function verification capability.

SI-7	Software, Firmware, and Information Integrity (High, Moderate)	Assurance	P1

Control:

The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information.

Supplemental 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, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Detection of unauthorized changes to sensitive information such as personally identifiable information (PII) and systems containing sensitive information is fundamental to ensuring integrity as required by the Privacy Act

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-4; HIPAA: 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(c)(2), 45 C.F.R. §164.312(e)(2)(i), 45 C.F.R. §164.312(c), 45 C.F.R.; NIST SP: 800-147, 800-155; Code: 5 U.S.C. §552a(e)(5); OMB Memo: M-04-04; OMB Circular A-130: 7.g., and Appendix II;	**Related Controls Requirement(s):** SA-12, SC-8, SC-13, SI-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Software integrity protection and verification capability.

SI-7(1)	Integrity Checks (High, Moderate)	Assurance	P1

Control:

The information system performs an integrity check of software, firmware, and information daily and at system startup.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, the organization reassesses the integrity of software and information by performing no less often than one monthly scans of the information system.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing software and information integrity; security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records.

SI-7(2)	Automated Notifications of Integrity Violations (High)	Assurance	P1

Control:

The organization employs automated tools that provide notification to defined personnel or roles (defined in the applicable System Security Plan) upon discovering discrepancies during integrity verification.

Supplemental Guidance:

The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business owners, information system owners, systems administrators, software developers, systems integrators, and information security officers.

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records.

SI-7(5)	Automated Response to Integrity Violations (High)	Assurance	P1

Control:

The information system automatically implements one or more of the security safeguards defined in Implementation Standard 1 when integrity violations are discovered. Implemented safeguards must be specified in the applicable System Security Plan.

Implementation Standards:

High:

Std.1 - One or more of the following safeguards must be implemented:
(a) Shuts the information system down;
(b) Restarts the information system; or
(c) Implements the security safeguards defined in the System Security Plan.

Supplemental Guidance:

Organizations may define different integrity checking and anomaly responses:
(i) By type of information (e.g., firmware, software, user data);
(ii) By specific information (e.g., boot firmware, boot firmware for a specific types of machines); or
(iii) A combination of both.
Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records.

SI-7(7)	Integration of Detection and Response (High, Moderate)	Assurance	P1

Control:

The organization incorporates the detection of defined unauthorized security-relevant changes (defined in the applicable System Security Plan) to the information system into the organizational incident response capability.

Supplemental 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 being able to identify and discern 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** IR-4, IR-5, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records.

SI-7(14)	Binary or Machine Executable Code (High)	P2

Control:

The organization:
a. Prohibits the use of binary or machine executable code from sources with limited or no warranty and without the provision of source code; and
b. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

Supplemental Guidance:

This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations.

Reference(s):	**Related Controls Requirement(s):** SA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing software and source code acquisition; information system design documentation; information system software component inventory; documentation of exceptions to the control's source code requirement; other relevant documents or records.
Interview: Organizational personnel with development and integration responsibilities.

SI-8	Spam Protection (High, Moderate)	P2

Control:

The organization:
a. Employs spam protection mechanisms at information system entry and exit points to detect and act on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental 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.

Guidance for systems processing, storing, or transmitting PHI:

HIPAA requires organizations to implement procedures for guarding against, detecting and reporting malicious software which can be introduced to the system through spam. Under the HIPAA Security Rule, this is an addressable implementation specification. HIPAA covered entities must conduct an analysis as described at 45 C.F.R. § 164.306 (Security standards: General rules) part (d) (Implementation specifications) to determine how it must be applied within the organization.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; HIPAA: 45 C.F.R.§164.308(a)(5)(ii)(B); 45 C.F.R.§164.308(a)(6)(ii) NIST SP: 800-45	**Related Controls Requirement(s):** 2, AT-3, SC-5, SC-7, SI-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Interview: Organizational personnel with spam protection responsibilities.
Test: Automated mechanisms implementing spam detection and handling capability.

SI-8(1)	Central Management (High, Moderate)	P2

Control:

The organization centrally manages spam protection mechanisms.

Supplemental Guidance:

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, centrally managed spam protection security controls.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AU-3, SI-2, SI-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.

SI-8(2)	Automatic Updates (High, Moderate)	P2

Control:

The information system automatically updates spam protection mechanisms.

Supplemental Guidance:

None.

Reference(s): FedRAMP Rev. 4 Baseline	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.

SI-10	Information Input Validation (High, Moderate)	Assurance	P1

Control:

The information system checks the validity of defined information inputs (defined in the applicable System Security Plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

Systems processing, storing, or transmitting PII (to include PHI):

The information system checks the validity of personally identifiable information (PII).

Supplemental 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Information input validation serves two important purposes for protecting PII:
(1) When PII is entered, validation techniques support data quality measures (e.g., ensuring the PII entered is the expected type and format of data); and
(2) It provides the capability to limit or exclude PII from being entered within a field (e.g., recognizing a restricted format, such as an SSN) that should not contain the PII.

Reference(s): FedRAMP Rev. 4 Baseline; FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; procedures addressing information validity; 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; other relevant documents or records.
Test: Information system capability for checking validity of information inputs.

SI-11	Error Handling (High, Moderate)	P2

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 System Security Plan).

Systems processing, storing, or transmitting PII (to include PHI):

The information system reveals error messages only to authorized individuals with a need for the information in the performance of their duties.

Implementation Standards:

Systems defined as CSPs:

High & Moderate:

CSP.1 - For CSPs, this Standard replaces the requirement defined within SI-11. The information system generates error messages that provide information necessary for corrective actions without revealing user name and password combinations; attributes used to validate a password reset request (e.g., security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings in error logs and administrative messages that could be exploited by adversaries.

Supplemental Guidance:

Organizations carefully consider the structure/content of error messages. The extent to which information systems can 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, 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

An error in a system may reveal sensitive information such as personally identifiable information (PIIP or protected health information (PHI). For example, if there is an error posting a form that contains PII and the system includes the PII entered in the form when it writes to the error log, it will be visible to whoever has access permissions to the error log. Therefore, error handling must be considered in design of the system, and access to errors containing leaked sensitive information should be provided only to those individuals with a need for that information in the performance of their duties.

Reference(s): Code: 5 U.S.C. §552a(e)(5) and (10); FedRAMP Rev. 4 Baseline; FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; OMB Circular A-130: 7.g.; 45 C.F.R. §164.308(a)(3)(i)	**Related Controls Requirement(s):** AU-2, AU-3, SI-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

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; other relevant documents or records.
Test: Information system error handling capability.

SI-12	Information Handling and Retention (High, Moderate, Low)	P2

Control:

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Systems processing, storing, or transmitting PII (to include PHI):

For personally identifiable information (PII) maintained in a Privacy Act system of records, the corresponding record management requirements, including retention periods, must be addressed in the system of records notice (SORN).

Implementation Standards:

High, Moderate, & Low:

Std.1 - Retain output, including but not limited to audit records, system reports, business and financial reports, and business records from the information system in accordance with CMS Policy and all applicable NARA requirements.

Systems processing, storing, or transmitting PHI:

PHI.1 - HIPAA requires that the following actions, activities, and assessments relating to the security of systems containing PHI be documented and retained for at least six years from the date of its creation or the date when it was last in effect, whichever is later:

• Decisions regarding addressable implementation specifications, specifically why it would not be reasonable and appropriate to implement the implementation specification in question;
• A user's right of access to a workstation, transaction, program, or process;
• Security incidents and their outcomes;
• Satisfactory assurances that a business associate will appropriately safeguard PHI. This documentation is recorded in a written contract or other arrangement with the business associate and must meet the applicable requirements of business associate agreements. If satisfactory assurances cannot be attained, document the attempt and the reasons that these assurances cannot be obtained;
• Repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks); and
• Changes to organizational policies and procedures.

Supplemental Guidance:

Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. NARA provides guidance on records retention.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Sensitive information such as PII, even if not considered a "record" by statute, should be handled and retained in accordance with applicable regulatory requirements, organizational policies, industry best practices, and the Fair Information Practice Principles (FIPP). Retention and handling of PII that meets the definition of a "record" as defined by the Federal Records Act (44 U.S.C. §3301) should be addressed in a records disposition schedule. For PII that meets the definition of a "record" as defined by the Privacy Act for purposes of providing notice, the associated SORN should reflect the retention period from the organization's applicable record retention schedule.
Protected health information (PHI) must be handled and retained in accordance with the HIPAA Security Rule as it has specific requirements for information handling and record retention.

Reference(s): Code: U.S.C. §552a(e)(4); FedRAMP Rev. 4 Baseline; FISCAM: BP-3; 44 U.S.C. §3301, 45 C.F.R. §164.316(b)(1)(ii); 45 C.F.R. §164.316(b)(2)(i)	**Related Controls Requirement(s):** AC-16, AU-5, AU-11, MP- 2, MP-4, AP-2, DM-2, TR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; 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.

SI-16	Memory Protection (High, Moderate)	P1

Control:

The information system implements security safeguards (e.g., data execution prevention, address space layout randomization) to protect its memory from unauthorized code execution. Implemented safeguards must be specified in the applicable system security plan.

Supplemental 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.

Reference(s): FedRAMP Rev. 4 Baseline	**Related Controls Requirement(s):** AC-25, SC-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: System and information integrity policy; system security plan; other relevant documents or records.
Interview: Organizational personnel with information system development responsibilities.

B.18 Program Management (PM)

PM-1	Information Security Program Plan (High, Moderate, Low)	P1

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, cyber-physical); and
4. Is approved by a senior official with responsibility and accountability for the risk being 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.

Supplemental Guidance:

Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans 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 implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.
The security plans for individual information systems and the organization-wide information security program plan together, 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 documents describing 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 the organizational official or officials 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 PE family when such controls are not associated with an information system but instead, support multiple information systems.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The organization's approach to protection of personally identifiable information (PII) should be included in the information security program plan, including defining roles and responsibilities for protecting PII.

Reference(s): Code: 5 U.S.C. §552a(e)(10); FISMA (Pub. L. No. 107-347); OMB Circular A-130, 7.g.; 45 C.F.R. §164.308 (a)(1)(i)	**Related Controls Requirement(s):** PM-8, AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; and other relevant documents or records.
Interview: Organizational personnel with security planning and plan implementation responsibilities for the information security program.

PM-2	Senior Information Security Officer (High, Moderate, Low)	P1

Control:

The organization appoints a Chief Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Implementation Standards:

Systems processing, storing, or transmitting PHI:

PHI.1 - The organization must designate privacy and security officials responsible for the development and implementation of the policies and procedures required by HIPAA (45 C.F.R. parts 160 and 164).

Supplemental Guidance:

The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

Guidance for systems processing, storing, or transmitting PHI:

Assigning security responsibilities to a senior official supports the HIPAA Security Rule.

Reference(s): OMB Memo: M-05-08; 45 C.F.R. §164.308(a)(2); 45 C.F.R. §164.530(a)	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; information security program plan; documentation addressing roles and responsibilities of the Chief Information Security Officer position; information security program mission statement; and other relevant documents or records.
Interview: CISO or designated representative.

PM-3	Information Security Resources (High, Moderate, Low)	P1

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/Exhibit 300/Exhibit 53 to record the resources required; and
c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance:

Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Ensuring that information security is adequately resourced supports the implementation of all security-related privacy requirements.

Reference(s): E-Government Act of 2002 (Pub. L. No. 107-347), §208; NIST SP: 800-65	**Related Controls Requirement(s):** PM-4, SA-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program 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; Exhibit 300; Exhibit 53; and other relevant documents or records.
Interview: Organizational personnel managing and overseeing the information security-related aspects of the capital planning and investment control process.

PM-4	Plan of Action and Milestones Process (High, Moderate, Low)	P1

Control:

The organization:
a. Implements a process for ensuring that plans of action and milestones 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 risk to organizational operations and assets, individuals, other organizations, and the Nation; and
3. Are reported in accordance with OMB FISMA reporting requirements and other applicable requirements, such as those within the FedRAMP.
b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance:

The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. 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. Plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

Reference(s): NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-02-01, M-14-03, M-15-01, M-16-04; 45 C.F.R. §164.310(d)	**Related Controls Requirement(s):** CA-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; plan of action and milestones policy; procedures addressing plan of action and milestones process; plan of action and milestones for the security program; plan of action and milestones for organizational information systems; other relevant documents or records.
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities

PM-5	Information System Inventory (High, Moderate, Low)	P1

Control:

The organization develops and maintains an inventory of its information systems, to include those operated on behalf of CMS (e.g., by a contractor, vendor, cloud service provider, or other service provider).

Supplemental Guidance:

This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.
OMB Circular NO A-130 Appendix III
The term “information system” means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Maintaining a current information system inventory supports privacy by informing personally identifiable information (PII) inventories, data flows, and generally assists in monitoring the maintenance and use of PII.

Guidance for systems processing, storing, or transmitting PHI:

Information system inventory should govern the receipt and removal of hardware and electronic media that contains PHI.

Reference(s):	**Related Controls Requirement(s):** SE-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Inventory of information systems.

PM-6	Information Security Measures of Performance (High, Moderate, Low)	P1

Control:

The organization develops, monitors, and reports on the results of information security measures of performance to evaluate the effectiveness of IT security and privacy policies, procedures, and controls. The measures and metrics must provide information on measures of implementation, efficiency, effectiveness, and impact.

Supplemental 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.

Reference(s): NIST SP: 800-55	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: List of monitored security measures of performance; reports providing results of security measure monitoring.
Examine: Verify that reported measures and metrics provide at least measures of implementation, efficiency, effectiveness, and impact for each measure of performance.
Interview: Organizational personnel with security performance measurement responsibilities

PM-7	Enterprise Architecture (High, Moderate, Low)	P1

Control:

The organization develops and implements an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Supplemental Guidance:

The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture (FEA). The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also 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 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. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

Reference the FEA Security and Privacy Profile for additional information.

Reference(s): Code: 5 U.S.C. §552a(e)(10); FISMA (Pub. L. No. 107-347); NIST SP: 800-39; OMB Circular A-130, 7.g.; Web: fsam.gov; 45 C.F.R. §164.308(a)(1)(i)	**Related Controls Requirement(s):** PL-2, PL-8, PM-11, RA-2, SA-3, AR-7

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Enterprise architecture design documentation; enterprise architecture implementation documentation; enterprise architecture requirements documentation; enterprise architecture risk assessment documentation; and other relevant documentation.
Interview: Organizational personnel with enterprise architecture design and/or conformance responsibilities

PM-8	Critical Infrastructure Plan (High, Moderate, Low)	P1

Control:

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance:

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.

Reference(s): NIST SP 800-34, 800-60	**Related Controls Requirement(s):** PM-1, PM-9, PM-11, RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; critical infrastructure and key resources protection plan; protection plan development documentation; other relevant documents or records.
Interview: Organizational personnel with critical infrastructure and key resources protection plan responsibilities.

PM-9	Risk Management Strategy (High, Moderate, Low)	P1

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 at least every three hundred and sixty-five (365) days or as required, to address organizational changes.

Systems processing, storing, or transmitting PII (to include PHI):

The risk management strategy must include a process to evaluate and address privacy risks for individuals and information (data) such as risk to individual, risk to the system, risk to the organization, and risk to the enterprise. In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.

Implementation Standards:

Systems processing, storing, or transmitting PHI:

PHI.1 - The risk management strategy must include a process to evaluate and address privacy risks for individuals and PHI such as risk to individual, risk to the system, risk to the organization, and risk to the enterprise. In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.

Supplemental Guidance:

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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

A comprehensive risk management strategy includes privacy as an input where appropriate to ensure privacy risks to individuals and organizations are identified, prioritized, and managed consistently across the organization's business processes, programs, and systems.

Reference(s): NIST SP: 800-30, 800-39; OMB Memo: M-03-22, M-06-16, M-17-12 Att. 1, B.1 and Att. 2, A.1; OMB Circular A-130, 7.g.; 45 C.F.R. §164.308(a)(1)(ii); 45 C.F.R. §164.316(a)	**Related Controls Requirement(s):** RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; risk management strategy documentation; evidence of consistent implementation of risk management strategy; samples of risk management documentation from disparate organizational information systems; other relevant documents or records.
Interview: Organizational personnel with risk management strategy responsibilities

PM-10	Security Authorization Process (High, Moderate, Low)	P1

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.

Systems processing, storing, or transmitting PII (to include PHI):

The organization's security authorization process must ensure privacy safeguards and privacy documentation requirements, such as privacy impact assessments (PIA) and systems of records notices (SORN) when applicable, have been appropriately addressed prior to any security authorization.

Implementation Standards:

Systems processing, storing, or transmitting PHI:

PHI.1 - The organization's security authorization process must ensure privacy safeguards and privacy documentation requirements have been appropriately addressed prior to any security authorization.

Supplemental 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 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The security authorization process provides a means for evaluating whether a system/process has met given privacy safeguards and documentation requirements.

Reference(s): Code: 5 U.S.C. §552a(e)(10); Pub. L. No. 107-347, §208; NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; OMB Circular A-130: 7.g. and 8.b.(3); 45 C.F.R. §164.308(a)(2)	**Related Controls Requirement(s):** CA-6, AR-2, AR-7, TR-1, TR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); and other relevant documents or records.
Interview: Organizational personnel with security authorization responsibilities for information systems; organizational personnel with risk management responsibilities.
Test: Organizational processes for security authorization; automated mechanisms supporting the security authorization process.

PM-11	Mission/Business Process Definition (High, Moderate, Low)	P1

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 achievable protection needs are obtained.

Systems processing, storing, or transmitting PII (to include PHI):

When defining mission/business processes for information security and identifying resulting risks, the organization must address the privacy risks stemming from those processes.

Supplemental 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. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.

Reference(s): FIPS Pub: 199; NIST SP: 800-60; OMB Circular A-130: 7.g. and 8.b.(1)(b), 8.b.(2)(b), and Appendix IV; 45 C.F.R. §164.306(a) and (b)	**Related Controls Requirement(s):** PM-7, PM-8, RA-2, AR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; mission/business process definitions; mission/business process risk assessment documentation; other relevant documents or records.
Interview: Organizational personnel with mission/business process definition responsibilities

PM-12	Insider Threat Program (High, Moderate, Low)	P1

Control:

The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

Systems processing, storing, or transmitting PII (to include PHI):

When defining the requirements for and designing an organization's insider threat program, the insider threat team must engage the participation, and obtain concurrence, of the organization's Privacy Officer prior to implementation. For existing insider threat programs, conduct a review of the program with the organization's Privacy Officer to ensure program meets applicable privacy requirements.

Implementation Standards:

High, Moderate, & Low:

Std.1 - As required by the CMS-EMP section of the CMS Information System Security and Privacy Policy (IS2P2), the organization implements the insider threat program in accordance with HHS Policy for Monitoring Employee Use of HHS IT Resources.

Supplemental Guidance:

Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. 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 department/agency 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 as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government- owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (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 department/agency insider threat posture.
Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

The privacy risks inherent with aggregating sensitive personally identifiable information (PII) from multiple data resources within an organization, such as human resource and background investigation information, and the potential for scope creep require the active participation, review, and concurrence of the Privacy Officer.

Reference(s): Code: 5 U.S.C. §552a(e)(5), (9), (10); E-Government Act of 2002 (Pub. L. No. 107-347), §208; Executive Order: 13587; HHS: Policy for Monitoring Employee Use of HHS IT Resources; OMB Memo: M-17-12; OMB Circular A-130: 7.g.	**Related Controls Requirement(s):** AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-1, PM-14, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; risk management policy; procedures addressing incident handling and response; and other relevant documents or records.
Interview: Organizational personnel with risk management responsibilities, organizational personnel with incident response responsibilities.

PM-13	Information Security Workforce (High, Moderate, Low)	P1

Control:

The organization establishes an information security workforce development and improvement program.

Supplemental 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:
a. Information security professionals to advance in the field and fill positions with greater responsibility; and
b. 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.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

To implement adequate security controls, the organization's information security and privacy workforce should be knowledgeable of the applicable privacy and security requirements commensurate with the level of access or responsibility for applying appropriate safeguards. The information security workforce should receive role-based training for the privacy requirements commensurate with the level of access or responsibility for applying safeguards to personally identifiable information (PII).

Reference(s): HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities; Code: 5 U.S.C. §552a(e)(9)-(10); OMB Memo: M-17-12; OMB Circular A-130: 7.g.; 45 C.F.R. §164.308(a)(2)	**Related Controls Requirement(s):** AT-2, AT-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; security workforce development and improvement program; security workforce development and improvement program procedures; and other relevant documents or records.
Examine: Information system implements automated information security and privacy role-based training/staff participation tracking.
Interview: Organizational personnel with risk management responsibilities, organizational personnel with security workforce development program responsibilities.

PM-14	Testing, Training, and Monitoring (High, Moderate, Low)	P1

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; and
2. Continue to be executed in a timely manner.
b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Systems processing, storing, or transmitting PII (to include PHI):

Reviews testing, training and monitoring plans for consistency with the organizational privacy risk management strategy.

Supplemental Guidance:

This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy and the widespread use of common controls, 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. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

It is critical to integrate privacy risk management, compliance monitoring, and testing into the organizational risk management strategy and the associated testing and training requirements otherwise an important aspect of privacy may be overlooked.

Reference(s): Code: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; HHS: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities; NIST SP: 800-16, 800-37, 800-115, 800-137; OMB Memo: M- 17-12 Att.1, A.2., M-14-03, M-15-01, M-16-04; OMB Circular A-130: 7.g.	**Related Controls Requirement(s):** AT-3, CA-7, CP-4, IR-3, SI-4, AR-4, AR-5, DM-3, SE-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; security testing, training, and monitoring process documentation; security testing, training, and monitoring activities procedures; and other relevant documents or records.
Interview: Organizational personnel with information security responsibilities.
Test: Automated mechanisms supporting development and maintenance of plans and processes for conducting security testing, training, and monitoring activities.

PM-15	Contacts with Security Groups and Associations (High, Moderate, Low)	P3

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.

Supplemental 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.

Reference(s): Code: 5 U.S.C. §552a; Pub. L. No. 107-347, §208; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; OMB Memo: M-17-12, M-05-08; OMB Circular A-130: 7.g.	**Related Controls Requirement(s):** SI-5, AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; security testing, training, and monitoring process documentation; security testing, training, and monitoring activities procedures; and other relevant documents or records.

PM-16	Threat Awareness Program (High, Moderate, Low)	P1

Control:

The organization implements a threat awareness program that includes a cross-organization information-sharing capability

Supplemental 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 that organizations have found are 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, 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.

Reference(s): Cybersecurity Enhancement Act of 2104	**Related Controls Requirement(s):** IR-10, PM-12

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Information security program policy; threat awareness program policy; threat awareness program procedures; and other relevant documents or records.
Interview: Security Operations personnel to verify the organization is actively participating in the threat awareness program of CMS. Verify that personnel act on threat information received from the CMS Cybersecurity Integration Center (CCIC) (and other external sources) as well as reporting threat information derived from investigations (or other external sources) to the CCIC.

B.19 Authority and Purpose (AP)

AP-1	Authority to Collect (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of specific programs and the needs of information systems.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

An organization identifies the legal authority permitting collection. Additional measures, including design choices, ensure the information system collecting, using, maintaining, or disseminating PII complies with those authorities permitting the collection.
Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Official for Privacy (SOP), 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), Privacy Impact Assessment (PIA), and/or other applicable documentation such as Privacy Act Statements, Notices of Privacy Practices, Website Privacy Policies, or Computer Matching Agreements. Ensure PII collected, used, maintained, or disseminated by the information system is related to, and compatible with, the purpose and scope of the authority described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.

Reference(s): Code: 5 U.S.C. §552a, Pub. L. No. 107-347, §208; E-Gov: §208(c); OMB Circular A-130: Appendix I; Privacy Act: §552a(e)	**Related Controls Requirement(s):** AR-2, DM-1, TR-1, TR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) 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
(ii) 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:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Legal authority 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.
Examine: SORN and/or PIA and verify that the legal authority is stated.

AP-2	Purpose Specification (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization, at the system or application level, describes the purpose(s) for which PII is collected, used, maintained, and shared in privacy compliance documentation, privacy notices, and privacy policies (e.g., PIAs, SORNs, Privacy Act Statements, and Computer Matching Agreements [CMAs]).

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

An organization identifies the authorized purpose(s) for collection, use, maintenance, or dissemination of PII. Additional measures, including, but not limited to, design choices and auditing, ensure the information system collecting, using, maintaining, or disseminating PII complies with those authorized purposes.
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 Senior Official for Privacy (SOP) 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.
Ensure the PII collected, used, maintained, or disseminated by the information system adheres to the specific purpose(s) described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.

Reference(s): Code: 5 U.S.C. §552a(e)(3)(A)-(B), Pub. L. No. 107-347, §208(b)(2)(B)(ii) and (c)(1)(B); E-Gov: §208(b), §208(c); Privacy Act: §552a(e)(3)(A)-(B)	**Related Controls Requirement(s):** AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices. Determine if:
(i) The system collects and uses PII only if the PII is relevant to its purposes;
(ii) PII entering the system from other systems is limited to predetermined data elements.
(iii) Generation of new PII is restricted to pre-determined data elements;
(iv) PII output is properly labeled regarding permissible uses and restrictions on usage of the PII;
(v) PII is transferred to other entities (e.g., other agencies or third parties) only if those entities are authorized to receive it and only for predetermined, documented purposes and business needs;
(vi) When transferring PII to other entities via the user interface, the system notifies the user of the permissible uses and restrictions on usage of the PII;(vi) When transferring PII to other agency systems or to third parties via the user interface, the system notifies the user of the permissible uses and restrictions on usage of the PII;
(vii) User interfaces provide a notification when saving PII outside the system or printing PII, reminding the user of the permissible uses and restrictions on usage of the PII; and
(viii) The system limits disclosure of PII to those data elements that are necessary for the purposes of the system.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Privacy notice that describes the purpose for which PII can be collected, used, maintained, and shared; other relevant documents or records.
Examine: System data model and database architecture and associate each PII data element or logical aggregate of elements (e.g., mailing address) with a rationale for its inclusion. Comment: Purpose Limitation is fundamentally system-specific. The implementation of this principle is heavily dependent on legal authorization and policy and could vary greatly for individual systems. Of the Enterprise Privacy Requirements, this is likely the most difficult for generating generic tests.
Examine: User interfaces in which PII is entered. Establish rationale for any unstructured capture mechanisms (e.g., free text boxes). Comment: Structured mechanisms for capturing PII input (e.g., discrete and appropriately formatted input fields for specific PII data elements) help constrain the PII that can be captured.
Examine: Display screens for evidence of appropriate warning. Comment: Unstructured data inputs pose a risk, as they are difficult to govern and users can enter any information they choose.
Examine: Interfaces to verify PII data elements being requested. Comment: Individual queries may also be executed. Volume of queries may drive the approach used. **Examine:** Interfaces to verify PII data elements being received. Comment: May also send full record to system, including unnecessary PII data elements. Unnecessary PII data elements may also be sent individually; however, it is likely more efficient/feasible to send a record that contains multiple types of elements that should not be accepted.
Examine: Output of each system function for PII data elements.
Test: Attempt to save a file or data extract from the system that contains PII.
Test: Attempt to print a file containing PII from the system. Comment: Notification may be handled in multiple ways, depending on the capabilities of the system, including screen views or pop-up notices.
Test: Create and save a file containing system output with PII and review the label associated with it. Comment: This requirement depends on system capabilities. When available, automated means of applying labels should be used.
Test: Print a file containing PII and review the label printed on it. Comment: Labels may include a file header or footer, a watermark, a designation in the file name, or some other means of communicating the authorized purpose.
Test: Create and save a file containing system output with PII. Attempt to alter the label that communicates the authorized use. Attempt to remove the label that communicates the

authorized use. Comment: When practical for the purpose, consider making electronic file outputs read-only.
Test: Submit a request to print a report containing PII. Attempt to alter the label that communicates the authorized use. Attempt to remove the label that communicates the authorized use.
Examine: Interfaces to verify that PII is being transferred to the intended systems.
Examine: Connection permissions for systems against the list of systems allowed to transfer PII out of the system.
Test: Attempt to connect from an unauthorized system and transfer PII out of the system.
Test: Attempt to initiate from system transfer of PII to an unauthorized system. Comment: Sharing agreements with other entities may include information documented in SORNs, information sharing agreements (ISA), memoranda of understanding (MOU), memoranda of agreement (MOA), and other formal agreements.
Test: Attempt to transfer PII from the system and observe any notification provided. Comment: Notification may be handled in multiple ways, depending on the capabilities of the system, including screen views or pop-up notices. Depending on business requirements, the system may also be required to support an acknowledgement of notice received by the user.
Examine: Target system updates to verify PII data elements being sent.
Test: Attempt queries from target systems for PII data elements not pre-determined to be necessary. Comment: Additional thought may be required when full records are being disclosed, including whether disclosure of the full record (instead of specific data elements) is compatible with the purposes of the system.

AP-CMS-1	Non-Mandatory: Authority and Purpose Control Family Policy and Procedures	Assurance	P3

Control:

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. An Authority and Purpose policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the Authority and Purpose policy and associated Authority and Purpose controls; and
b. Reviews and updates (as necessary) the current:
1. Authority and Purpose policy at least every two (2) years; and
2. Authority and Purpose procedures at least every two (2) years.

Implementation Standards:

High & Moderate:

Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AP family. Policy and procedures reflect applicable federal laws, Executive Orders, 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 program in general and for information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): E-Gov: §208(b), §208(c); OMB Circular A-130: Appendix I; Privacy Act: §552a(e)	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Authority to collect policy and procedures, and other relevant documents.
Interview: Organizational personnel with authority to collect responsibilities, ensure responsibilities are acknowledged.

B.20 Accountability, Audit, and Risk Management (AR)

AR-1	Governance and Privacy Program (High, Moderate, Low)	P1

Control:

The organization:

a. Appoints a Senior Official for Privacy (SOP) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;
b. Monitors federal privacy laws and policy for changes that affect the privacy program;
c. Allocates an appropriate allocation of budget and staffing resources to implement and operate the organization-wide privacy program;
d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
f. Updates privacy plan, policies, and procedures, as required to address changing requirements, but no less often than every two years.

Implementation Standards:

High & Moderate:

Std.1 - Development of the strategic organizational privacy plan must be done in consultation with the CMS CIO and CISO. The organization establishes and institutionalizes contact for its privacy professionals with selected groups and associations within the privacy community:
(a) To facilitate ongoing privacy education and training for organizational personnel;
(b) To maintain currency with recommended privacy practices, techniques, and technologies; and
(c) To share current privacy-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance:

Effective implementation of privacy and security controls requires a collaborative partnering of the SAOP (or Chief Privacy Officer [CPO]), CIO, and CISO. To maximize organizational compliance with privacy requirements and best practices, the organization should ensure its privacy professionals engage with both its security community and the Federal privacy community to remain current and to share lessons-learned or other privacy-related information.
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 SOP with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SOP, 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 SOP 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 SOP. 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 Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix 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.
Ongoing contact with privacy groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Privacy groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of privacy 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.

Guidance for Systems processing, storing, or transmitting PHI:

HIPAA requires policies, procedures, and personnel designations to be documented and for organizations to monitor changes in law.

Reference(s): CFR: 45 C.F.R. §164.530(a)(1)(i), 45 C.F.R. §164.530(i)(1), (2), and (3); Code: 44 U.S.C.: §3541, 5 U.S.C. §552a, 44 U.S.C. §3506 (a)(3) and (g), Pub. L. No. 107-347, §208; OMB Memo: M-03-22, M-05-08, M-17-12; OMB Circular A-130; Privacy Act: §552a	**Related Controls Requirement(s):** AP-CMS-01, AR-CMS-01, DI-CMS-01, DM-CMS-01, IP-CMS-01, TR-CMS-01, UL-CMS- 01, PM-15

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization appoints a Senior Official for Privacy (SOP) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;
(ii) The organization monitors federal privacy laws and policy for changes that affect the privacy program;
(iii) The organization allocates an appropriate allocation of budget and staffing to implement and operate the organization-wide privacy program;
(iv) The organization develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
(v) The organization 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
(vi) The organization updates privacy plan, policies, and procedures, as required to address changing requirements, but at least every two years.

Assessment Methods and Objects:

Examine: Organizational governance and privacy policy; governance and privacy program plan; governance and privacy procedures; budget and staffing documentation; strategic organizational privacy plan; privacy policies and procedures; information system privacy and security controls; other relevant documents or records.
Interview: Organizational person appointed to the senior privacy officer/official position.

AR-2	Privacy Impact and Risk Assessment (High, Moderate, Low)	P1

Control:

The organization:
a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII;
b. Conducts PIAs for information systems, programs, electronic information collections, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures; and
c. Reviews the PIA no less than every three (3) years and publishes the PIA in accordance with HHS guidance.

Supplemental Guidance:

Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the organization's mission, business processes, and information systems. Privacy Impact Assessments (PIAs) are structured reviews (qualitative and quantitative) of both the risk and effect of how information is handled and maintained as well as the potential impacts or harms to individuals and organizations for loss of control or mishandling of the PII. The term "PIA" may refer to the process of conducting such an assessment, or the document produced as a result of that assessment. A PIA-like process benefits an organization and the individuals whose PII is in the information system by enabling the organization to identify, evaluate, and manage the privacy risks for the PII in that system.
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. Such tools include, but are not limited to, conducting PIAs. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on the timing for developing PIAs for information systems and electronic collections of information. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.
Information system privacy risk management processes operate across the life cycle of an information system collecting, using, maintaining, and/or disseminating PII. Such privacy risk management processes include, but are not limited to, design requirements, privacy threshold analysis, privacy impact assessments (PIA), and implementation of secure disposition.
While Section 208 of the E-Government Act does not require — or prohibit — a PIA for a national security system (NSS), as defined at 40 U.S.C. §11103 (see Section 202(i) of the E-Government Act), an organization may benefit from conducting a PIA or similar privacy risk evaluation on NSS as part of their internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing PII. For this reason, the ARS extends the requirement to develop a PIA to all information systems.

Reference(s): CFR: 45 C.F.R. §164.530(c); Code: 44 U.S.C.: §3541; E-Gov: §208; OMB Memo: M-03-22, M-05-08, M-10-23; OMB Circular A-130: 7.g., 8.a.(1), 8.b.(2), and 8.b.(3)	**Related Controls Requirement(s):** RA-3

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmission, use, and disposal of PII; and
(ii) The organization conducts PIAs for information systems, programs, or other activities in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.
Determine if the privacy controls and protection of PII have been considered in the information security risk assessment (ISRA). Determine if:
(i) The system's security controls are based on a confidentiality impact level equal to or greater than the PII confidentiality impact level.

Assessment Methods and Objects:

Examine: Privacy risk management planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records.
Interview: Interview the Information System Security Officer (ISSO) and/or the Business Owner to determine if the privacy controls and protection of PII have been considered in their ISRA. Ensure the organization has a finalized privacy impact assessment (PIA) that has been signed within the last three years.
Examine: PII and system confidentiality impact levels and compare the two.
Examine: Final PIA and confirm that PIA is published on HHS website.

AR-3	Privacy Requirements for Contractors and Service Providers (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:
a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers;
b. Includes privacy requirements in contracts and other acquisition-related documents; and
c. Reviews, every two (2) years, a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, to ensure that the contracts include clauses that make all requirements of the Privacy Act apply to the system and that make the criminal penalty provisions of the Privacy Act apply to the contractor or service provider and its personnel.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High:

PRIV.1- The contract or other acquisition-related documents must flow-down privacy and security clauses to ensure sub-contractors adequately protect personally identifiable information (PII).

Moderate:

PRIV.1- The contract or other acquisition-related documents must flow-down privacy and security clauses to ensure sub-contractors adequately protect PII.

Systems processing, storing, or transmitting PHI:

PHI.1 - Under HIPAA, a business associate must ensure its contracts or other arrangements with subcontractors meet the requirements of 45 §C.F.R. §164.504(e)

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Contracts and other acquisition-related documents provide an enforceable means to ensure privacy and security controls are provided for PII shared with or disclosed to recipients outside of the organization, such that contractors and service providers protect PII in the same way the organization does.
Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Official for Privacy (SOP), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.

Reference(s): CFR: 48 C.F.R. Part 24.102, 48 C.F.R. Part 39.105, 45 C.F.R. §164.504(e); 45 C.F.R. §164.530(c); Code: 5 U.S.C. §552a(m); FAR: Part 24; OMB Circular A-130: 7.g.; Privacy Act: §552a(m)	**Related Controls Requirement(s):** AR-1, AR-5, SA-4

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:

(i) The organization establishes privacy roles, responsibilities, and access requirements for contractors and service providers;
(ii) The organization includes privacy requirements in contracts and other acquisition-related documents; and
(iii) The organization has documented procedures regarding privacy requirements for contractors or service providers and are implemented as described.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization privacy policy establishing privacy roles, responsibilities, and access requirements for contractors and service providers; privacy requirements in contracts and other acquisition-related documents; other relevant documents or records.

AR-4	Privacy Monitoring and Auditing (High, Moderate, Low)	P1

Control:

The organization

a. Monitors and audits privacy controls no less often than once every 365 days to ensure effective implementation; and
b. Monitors for changes to applicable privacy laws, regulations, and policy affecting internal privacy policy no less often than once every 365 days to ensure internal privacy policy remains effective; and
c. Documents, tracks, and ensures mitigation of corrective actions identified through monitoring or auditing.

Supplemental Guidance:

Monitoring and auditing activities ensure privacy controls are implemented and operating effectively.

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 [800-53 Appendix J], organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).

Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The Senior Official for Privacy (SOP) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials.

Where security and privacy controls align, to achieve the most efficient and effective implementation, the CMS SOP/CPO and CIO or CISO should coordinate to develop a single organizational process to conduct audit and monitoring.

Reference(s): Code: 44 U.S.C.: §3541; E-Gov: §208; OMB Memo: M-03-22, M-05-08, M-06-16, M-17-12; OMB Circular A-130; Privacy Act: §552a; 45 C.F.R. §164.530(a)(1)(ii)	**Related Controls Requirement(s):** AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization monitors and audits privacy controls and internal privacy policy as required to confirm effective implementation. Determine if the system captures all requests to update personally identifiable information (PII) in the system and when the update has been completed
Determine if the system is equipped with mechanisms to produce trend and comparative analysis on the manipulation of PII, for systems that generate their own analysis of PII.
Determine if the system reports on inappropriate manipulation of PII.
Determine if the system recognizes established thresholds that when met signify suspicious user activity. Determine if the system notifies the user, administrator, or other relevant party of any failure during transfer of PII. Determine if the system maintains an audit log of attempts to produce new PII.
Determine if the organization tracks the storage and access of PII.
Determine if the PII is restricted to "need to know" and removed when no longer required.

Assessment Methods and Objects:

Examine: Organization privacy policy monitoring and auditing requirements; internal privacy policy to confirm effective privacy control implementation; procedures for monitoring and auditing privacy controls; audit controls and records; other relevant documents or records.
Examine: Review audit log that provides evidence of PII being updated in the system to verify its existence.
Test: Submit updated test PII to the system.
Test: Attempt to generate report on the total number of times updated PII was submitted to the system and the data fields updated within a specified time period. Comment: Comparative analysis may include frequency of requests to and action of updating PII, common data fields updated, and peak periods for these occurrences.
Examine: Review function that generates trend and comparative analysis on newly produced or input PII. Comment: If the system interface is highly constrained, where users and their degrees of freedom are predetermined, then technically this requirement should be a non-issue. Conversely, if users' freedoms are not predetermined and less controlled, then this requirement becomes more relevant.
Examine: Review the system's design documentation for reporting function for system anomalies.
Examine: Review the system's design documentation for analysis function
Test: Attempt to engage in a behavior (e.g., user excessively accessing records) that might indicate inappropriate use of PII.
Test: Initiate a data transfer to an authorized system and introduce an interruption that will cause the transfer to fail. Observe any alerts produced by the system. Comment: Transfer failures can result in incomplete records for individuals. Examples of failures to introduce would be to disconnect one of the test systems from the network, attempt to connect to a destination system that will not allow a connection from the system being tested, or writing to a full drive. Notifications may include on-screen alerts, log entries, or some other method.
Examine: Review audit log that shows evidence of new PII produced. Comment: If the system interface is highly constrained, where users and their degrees of freedom are predetermined, then technically this requirement should be a non-issue. Conversely, if users' freedoms are not predetermined and less controlled, then this requirement becomes more relevant.
Interview: Interview the Information System Security Officer (ISSO)/Privacy Officer to determine how the organization tracks the storage and access of PII.
Examine: Request and examine documentation describing the lifecycle of collected PII to determine if the PII is restricted to "need to know" and removed when no longer required.
Examine: Examine any physical documents containing PII, and review records of monitoring and disposition.

AR-5	Privacy Awareness and Training (High, Moderate, Low)	P1

Control:

The organization:
a. Develops, implements, and updates a comprehensive privacy training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
b. Administers basic privacy training no less often than once every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII no less often than once every three hundred sixty-five (365) days; and
c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements no less often than once every three hundred sixty-five (365) days.

Implementation Standards:

High, Moderate, & Low:

Std.1 – A privacy education and awareness training program must be developed and implemented for all employees and individuals working on behalf of CMS involved in managing, using, and/or processing PII.
Std.2 - Privacy education and awareness training must include responsibilities associated with sending PII in email.
Std.3 - Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities.
Std.4 - Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to organization information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities.
Std.5 - Additional or advanced training must be provided commensurate with increased responsibilities or change in duties.
Std.6 - Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed.
Std.7 - Training must address the rules for telework and other authorized remote access programs.

Supplemental Guidance:

Privacy Training is an effective means to reduce privacy risk for an organization and is mandated by the Privacy Act of 1974, as amended, and OMB M-17-12.
Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. 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 Privacy Impact Assessments (PIA) or System of Records Notices (SORN) 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.
Privacy training may be integrated with general IA training. Examples of jobs or roles that would require job-specific privacy and security training include: human resource personnel who have greater access to PII; system developers who design, develop and implement information systems containing PII; and system administrators who operate and maintain information systems containing PII.

Reference(s): Act: Telework Enhancement Act of 2010; CFR: 45 C.F.R. §164.530(b)(1), 45 C.F.R. §164.530(a)(1)(ii); Code: 5 U.S.C. §552a(e)(9), 44 U.S.C.: §3541, Pub. L. No. 107-347, §208, Pub. L. No. 107-347, Title III; E-Gov: §208; OMB Memo: M-03-22, M-05-08, M-06-16, M-17-12, Att. 1, A.2.d.; OMB Circular A-130:; Privacy Act: §552a(e); HHS IRM Policy for IT Security for Remote Access; Master Labor Agreement	**Related Controls Requirement(s):** AR-3, AT-2, AT-3, TR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
(ii) The organization administers basic privacy training at least every 365 days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII at least every 365 days;
(iii) The organization ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least every 365 days; and
(iv) The organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods and Objects:

Examine: Training and awareness policy; training and awareness program plan strategy; privacy and awareness training material; training records; other relevant documents or records.
Examine: Privacy role-based training and compliance tracking mechanisms.
Interview: Organizational personnel with privacy training responsibilities.
Interview: A sample of system users.

AR-6	Privacy Reporting (High, Moderate, Low)	P1

Control:

The organization develops, disseminates, and updates reports to 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.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - The CCIC provides oversight of information security and privacy, to include privacy reporting, for each FISMA System operating by or on behalf of CMS.

Supplemental Guidance:

Privacy reporting helps organizations to determine progress in meeting privacy compliance requirements and to ensure organizational accountability. Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the Federal Government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Official for Privacy (SOP) reports to OMB; (ii) reports to Congress

required by the Implementing Regulations of the 9/11 Commission Act; or (iii) other public reports required by specific statutory mandates or internal policies of organizations. The SOP consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Guidance for Systems processing, storing, or transmitting PHI:

HIPAA covered entities have specific reporting requirements to the Secretary, Health and Human Services.

Reference(s): CFR: 45 C.F.R. §160.310(a); 45 C.F.R. §164.408; Code: 5 U.S.C. §552a, 44 U.S.C. §3541(4), 44 U.S.C. §3541, Pub. L. No. 107-347, §208; 9/11 Comm Act: §2000ee-1, Section 803, §2000ee-3, Section 804; Consolidated Appropriations Act: §522; E-Gov: §208; OMB Memo: M-08-09; OMB Circular A-130: 7.g.; Privacy Act: §552a	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:
(i) The organization develops privacy reports to 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;
(ii) 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;
(iii) The organization updates privacy reports within the time period specified by specific statutory and regulatory privacy program mandates but no less than within every three hundred sixty-five (365) days; and
(iv) The organization meets all the requirements specified in the applicable Implementation Standard(s).

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: Organizational personnel with information security and privacy responsibilities.

AR-7	Privacy-Enhanced System Design and Development (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization designs information systems to support privacy by automating privacy controls to the extent feasible, integrating and meeting privacy requirements throughout the CMS Life Cycle, and incorporating privacy concerns into reviews of significant changes to HHS/CMS systems, networks, physical environments, and other agency infrastructures. The organization also conducts periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act, the organization's privacy policy, and any other legal or regulatory requirements.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Automating privacy controls provides a concrete way of ensuring information systems are behaving in a way that is intended to achieve privacy objectives. Implementation of this control enables organizations to automate application of privacy controls. One simple example, which many organizations have already implemented, is TR-1, "Privacy Notice." This concept is one part of the most commonly recognized approaches to "building privacy in," which is sometimes also known as "Privacy by Design." Privacy by Design is an internationally accepted privacy best practice endorsed by the Federal Trade Commission in their March 2012 Final Report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," and embodies the same principles of the Privacy Act and Section 208 of the E-Government Act requiring privacy protections and safeguards before establishing or operating a system that may contain PII. Privacy by Design calls for considering privacy risks in the design and management of information systems. In addition to building in security and privacy controls discussed throughout the ARS, this control considers additional privacy-specific system characteristics and controls that must be built into the system to address privacy risks.

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 personally identifiable information (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 Privacy Act and the organization's privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes.

Additional guidance on privacy-enhanced design and development may be found in the HHS Enterprise Performance Lifecycle (EPLC).

Regardless of the systems engineering lifecycle used, privacy requirements should be considered during system design and development and validated and verified along with other system requirements. Validation ensures the correct requirements were identified. Verification ensures the requirements were implemented correctly.

Reference(s): CFR: 45 C.F.R. §164.530(c); Code: 5 U.S.C. §552a, Pub. L. No. 107-347, §208; E-Gov: §208(b), §208(c); OMB Memo: M-03-22, M-17-12; OMB Reports: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, Federal Trade Commission Final Report (March 2012); Privacy Act: §552a(e)(10)	**Related Controls Requirement(s):** AC-6, AR-4, AR-5, DM-2, TR-1, SA-3, SA-8

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization designs information systems to support privacy by automating privacy controls. Determine if:
(i) The system's technical monitoring and reporting functionalities are consistent with those described in the system's privacy compliance documents;
(ii) PII data fields are properly tagged as PII, for systems with supporting technology;
(iii) PII transferred to other systems is transferred with proper tagging of data fields, for systems with supporting technology; and
(iv) Views of PII are defined for each distinct user and/or target system role

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Information system design documentation; other relevant documents or records.
Examine: The application of technical monitoring and reporting functionalities in the system to confirm that they match technical functionalities described in the system's privacy impact assessment (PIA), system of records notice (SORN), and any other privacy compliance documents that describe this information.
Examine: Database schema to confirm that PII data elements are tagged as such and that other data elements are not tagged as PII.
Examine: Data fields within the database to confirm that PII data elements are tagged as such and that other data elements are not tagged as PII.
Test: Attempt to transfer data to an authorized system. Review the way the target system handles the data field tags for PII. Comment: This test is outside the boundary of the system tested; however, it is a critical step in the use of data tagging and must be considered. Metadata should be included in this review and may be the primary means for meeting this requirement. Metadata may provide information such as time/date stamps, purposes of the PII, and other valuable information about the data.
Examine: System design documentation to view template design.
Test: Logon to the system as test users with differing roles to verify that viewable PII is consistent with roles. **Test:** Log into the system as test users with differing roles to verify that views are consistent with roles **Examine:** System functions used to generate reports.
Examine: Access controls for user accounts and target system connections.

AR-8	Accounting of Disclosures (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

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 (5) 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.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Both the Privacy Act and HIPAA require accountings of disclosures in certain circumstances. There are differences in the requirements to account for disclosures under the Privacy Act and under HIPAA.
The Senior Official for Privacy (SOP), periodically consults with managers of their organization's systems of records to ensure that 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.

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

HIPAA covered entities have specific accountings of disclosure requirements. An accounting of disclosure documents the disclosures of PHI made by the organization to third parties. Not all disclosures are required to be reported. For specific accounting disclosure requirements see 45 C.F.R. §164.528.

Reference(s): CFR: 45 C.F.R. §164.528; Code: 5 U.S.C. §552a(c), (j), and (k); Privacy Act: §552a(c)(1), §552a(c)(3), §552a(j), §552a(k)	**Related Controls Requirement(s):** IP-2

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
a. The organization retains the accounting of disclosures for the life of the record or five (5) years after the disclosure is made, whichever is longer; and
b. The organization makes the accounting of disclosures available to the person named in the record upon request. Determine if:
(i) Exchanges between the system and third parties of personally identifiable information (PII) must be accounted for by formal documentation (e.g., privacy impact assessment [PIA], memorandum of understanding [MOU], information sharing agreement [ISA]); and
(ii) The system logs the date, purpose, and to whom the record was disclosed, for systems that maintain an accounting of disclosures under sub-section (c) of the Privacy Act.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Records documenting the disclosures of information held in each system of records under its control; retention policy for the disclosure records; policy for making the disclosures available to the person named in the record upon request; other relevant documents or records.
Interview: Interview the Information System Security Officer (ISSO) and/or Business Owner to ensure they are recording disclosures of privacy information when and if they occur. Request to view records of the disclosures, as appropriate.
Examine: Alignment between authorized system connections and system interface configurations to ensure that the system is interfacing only with authorized third party systems.
Examine: Applicable authorization agreement(s) against PII exchanges between the system and third parties to verify that data exchanges are authorized.
Examine: The system's design documentation to verify there is a function responsible for capturing information pertaining to disclosure activity.
Test: Disclose PII from the system to a target entity to verify that the disclosure is logged. Comment: Subsection (c) of the Privacy Act requires the agency to keep an accurate account of when and to whom it has disclosed PII. This includes the date, nature, and purpose of each disclosure of a record.

AR-CMS-1	Non-Mandatory: Accountability, Audit, and Risk Management Control Family Policy and Procedures	Assurance	P3

Control:

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. An Accountability, Audit, and Risk Management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the Accountability, Audit, and Risk Management policy and associated Accountability, Audit, and Risk Management controls.
b. Reviews and updates (as necessary) the current:
1. Accountability, Audit, and Risk Management policy at least every two (2) years or when there has been a significant change in applicable privacy laws, regulations, and policy affecting internal privacy policy; and
2. Accountability, Audit, and Risk Management procedures at least every two (2) years or when there has been a significant change in applicable privacy laws, regulations, and policy affecting internal privacy policy.

Implementation Standards:

High:

Std.1 - The SSP must document this control family. If the system does not contain PII or PHI, the controls within this family must be documented as "Limited Applicability - System does not process PII nor PHI."

Moderate:

Std.1 - The SSP must document this control family. If the system does not contain PII nor PHI, the controls within this family must be documented as "Limited Applicability - System does not process PII nor PHI."

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AR family. Policy and procedures reflect applicable federal laws, Executive Orders, 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 program in general and for information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): Code: 44 U.S.C.: §3541; E-Gov: §208; FAR: Part 24; OMB Memo: M-03-22, M-05-08, M-06-16, M-17-12, M-10-23; OMB Circular A-130; Privacy Act: §552a	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Accountability, audit, and risk management policy and procedures, and other relevant documents.
Interview: Organizational personnel with accountability, audit, and risk management responsibilities, ensure responsibilities are acknowledged.

B.21 Data Quality and Integrity (DI)

DI-1	Data Quality (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:

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

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

When a record is used to make determinations related to a right, benefit, or privilege for an individual, the Privacy Act of 1974, as amended, requires the information used be accurate, relevant, timely, and complete to assure fairness to the individual in the determination. Agencies should ensure the quality of all its PII, even if it is not protected by the Privacy Act. Organization's data quality assurance process should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, 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., a patient's health data), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

When PII is of a sufficiently sensitive nature (such as, but not limited to, when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit or adjudication of an employee's clearance), organizations should incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be confirmed accurate, relevant, timely, and complete. Frequency of confirmation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Reference(s): Code: 5 U.S.C. §552a(e)(5;); OMB Memo: M-17-12; OMB Circular A-130: Appendix I, 7.g. and 8.a.9; Paperwork Reduction Act, 44 U.S.C. §3501; Privacy Act: §552a(c), §552a(e), §552a(a)(8)(A), §552a(o), §552a(p), §552a(u); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C §515, 114 Stat. 2763A-153-4	**Related Controls Requirement(s):** AP-2, DI-2, DM-1, IP-3, SI- 10

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:

(i) The organization confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;
(ii) The organization collects PII directly from the individual to the greatest extent practicable;
(iii) The organization checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the Data Integrity Board; and
(iv) The organization issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. Determine if:
(i) The system ensures that multiple instances of the same PII data elements do not deviate unacceptably in their values;
(ii) The system checks time sequenced PII to ensure correct sequencing;
(iii) The system checks received PII for type and format consistency;
(iv) The system checks PII date thresholds to detect outdated PII and to alert the user;
(v) The system recognizes and alerts the user when PII is not sufficiently complete to adequately accomplish the intended purposes of the system; and

(vi) PII collected directly from the individual takes precedence over PII collected from third parties.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization privacy policy; privacy program plan; privacy program procedures; guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information; other relevant documents or records.
Examine: All instances where the test PII data elements appear in the system.
Test: Enter incorrectly sequenced PII into the system and observe any warnings provided. Comment: The exact nature of what is tested is highly system dependent.
Test: Submit a numeric value for an alphabetic field and an alphabetic value for a numeric field.
Test: Submit an alpha-numeric PII element to the system that is incompatible with the length or format expected.
Test: Submit test PII that is not logically consistent (e.g., date of birth [DoB] and age do not match) to the system and observe any warnings. Comment: The exact nature of what is tested is highly system dependent.
Test: Submit test PII to the system that is out of date for the intended purposes and observe any warnings.
Test: Submit test PII that does not meet the established level of completeness to the system and observe any warnings. Comment: The exact nature of what is tested is highly system dependent.
Test: Submit test PII collected as a third-party source and the same test PII collected from the individual to the system with variations in the two PII submissions. Comment: Applies to systems where similar PII element(s) gathered from both the individual and one or more third party sources are collected, processed, or propagated, and where the PII from either source may be used to accomplish the purposes of the system.

DI-1(1)	Validate PII (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization requests that the individual or individual's authorized representative validate PII during the collection process.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Validating PII that is used to determine a right, benefit, or privilege for an individual ensures the determination is based on accurate, timely, and relevant information. Procedures for validating PII should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.
When PII is of a sufficiently sensitive nature (such as, but not limited to, when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit or adjudication of an employee's clearance), organizations incorporate mechanisms into information systems and develop corresponding procedures and methods to validate the PII is accurate, relevant, timely, and complete.

Reference(s): Code: 5 U.S.C. §552a(e)(5;); OMB Circular A-130: 7.g. and 8.a.9.	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization requests that the individual or individual's authorized representative validate PII during the collection process.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization privacy policy; privacy program plan; privacy program procedures; PII validation procedures; other relevant documents or records.

DI-1(2)	Re-Validate PII (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate no less often than once every 365 days or as directed by the Data Integrity Board.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Revalidation must occur as frequently as is necessary to ensure the PII is accurate, relevant, timely, and complete; commensurate with the impact of the determination to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Re-validation of PII used to determine a right, benefit, or privilege for an individual, is necessary to ensure the determination is based on the most accurate, timely, and relevant information. Frequency of revalidation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Reference(s): Code: 5 U.S.C. §552a(e)(5;); OMB Circular A-130: 7.g. and 8.a.9;	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate as directed by the Data Integrity Board.
Determine if the system prompts the user to revalidate the PII collected.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization privacy policy; privacy program plan; privacy program procedures; PII validation procedures; other relevant documents or records.
Examine: If the system collects and stores PII, test the process to confirm it prompts the user to revalidate the PII collected.

DI-2	Data Integrity and Data Integrity Board (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:
a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and
b. Establishes a Data Integrity Board(DIB) when appropriate to oversee organizational CMA and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

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. CMS coordinates with the HHS Data Integrity Board. The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under CMAs.

Reference(s): Code: 5 U.S.C. §552a(a)(8), (o), and (u); OMB Circular A-130: Appendix I; Privacy Act: § 552a(a)(8)(A), § 552a(o), § 552a(p), § 552a(u);	**Related Controls 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

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The organization documents processes to confirm the integrity of PII through existing security controls; and
(ii) The organization establishes a Data Integrity Board when appropriate to oversee organizational computer matching agreements (CMA) and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization PII integrity policy; PII integrity program plan; PII integrity process and procedures; system security plan; other relevant documents or records
Examine: Review system security plan (SSP) to confirm PII data integrity is documented.

DI-2(1)	Publish Agreements on Website (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization publishes CMAs on its public website.

Supplemental Guidance:

None.

Reference(s): Code: 5 U.S.C. § 552a (a)(8)(A), (o), (p), (u);	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization publishes Computer Matching Agreements on its public website.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization CMAs; other relevant documents or records.
Examine: Request the locations where CMAs are intended to be published and verify CMAs are posted on the public website, if applicable. CMS publishes agreements on its public website at http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/ComputerMatchingAgreements.html

DI-CMS-1	Non-Mandatory: Data Quality and Integrity Control Family Policy and Procedures	Assurance	P3

Control:

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. Data Quality and Integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the Data Quality and Integrity policy and associated Data Quality and Integrity controls; and
b. Reviews and updates (as necessary) the current:
1. Data Quality and Integrity policy within every two (2) years; and
2. Data Quality and Integrity procedures within every two (2) years.

Implementation Standards:

High & Moderate:

Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the DI family. Policy and procedures reflect applicable federal laws, Executive Orders, 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 program in general and for information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): OMB Memo: M-17-12; OMB Circular A-130: Appendix I; Paperwork Reduction Act, 44 U.S.C. §3501; Privacy Act: §552a(c), §552a(e), §552a(a)(8)(A), §552a(o), §552a(p), §552a(u); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C §515, 114 Stat. 2763A-153-4	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Data quality and integrity policy and procedures, and other relevant documents.
Interview: Organizational personnel with data quality and integrity responsibilities to ensure responsibilities are acknowledged.

B.22 Data Minimization and Retention (DM)

DM-1	Minimization of Personally Identifiable Information (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:

a. Identifies the minimum PII elements that are relevant and necessary to accomplish the purpose of collection (and where a collection of certain PII requires legal authorization, HHS/CMS must ensure that such collection is legally authorized);
b. Limits the collection and retention of PII to the minimum elements identified in the notice and, when the collection of PII is made directly from the subject individual, limits its purposes to those for which the individual has provided consent to the extent permitted by law; and
c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, no less often than once every three hundred sixty-five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Coordinating review of the organization's holdings of PII with existing system review processes maximizes the efficient use of organization resources and will ensure all PII retained, even if the PII is not maintained in a Privacy Act system of records, is relevant and accurate. Reducing PII to the minimum required to accomplish the legally authorized purpose of collection and retaining PII for the minimum necessary period of time reduces the risk of PII breaches and will reduce the risk of the organization making decisions based on inaccurate PII.
Organizations take appropriate steps to ensure that 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's business process may be a subset of the PII the organization is authorized to collect. Program officials and program representatives such as Data Guardians consult with the Senior Official for Privacy (SOP) 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 17-12 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 NARA retention schedules.
Organizations should coordinate the PII holdings reviews with the systems' annual information security reviews schedule to the maximum extent practicable.
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.

Reference(s): CFR: 45 C.F.R. §164.502(b); Code: 5 U.S.C. §552a(e)(1); E-Gov: §208(b); OMB Memo: M-03-22, M-17-12; OMB Circular A-130: 7.g. and 8.a.; Privacy Act: §552a(e)	**Related Controls Requirement(s):** AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The organization identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
(ii) 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;
(iii) The organization conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, at least every 365 days, to confirm 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.
Determine if the system's intake of PII is consistent with the privacy notices related to the system, including System of Records Notice (SORN), Privacy Impact Assessment (PIA), and notices provided at points of collection.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization privacy data minimization and retention policy; privacy data minimization and retention program plan; privacy data minimization and retention program procedures; PII holding evaluation and review documentation; other relevant documents or records.
Examine: Documented system inputs with relevant privacy notices. Comment: Types and breadth of notice provided may vary widely by system. Testers must consult with relevant offices to confirm an accurate understanding of notice statements.

DM-1(1)	Locate/Remove/Redact/Anonymize PII (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization, where feasible and within the limits of technology and the law, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit authorized use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

NIST SP 800-122 provides guidance on anonymization.

Reference(s): NIST SP: 800-122;	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

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:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization privacy data anonymization and de-identification policy; privacy data anonymization and de-identification policy procedures; other relevant documents or records.

DM-2	Data Retention and Disposal (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:
a. Retains each collection of PII for the time period specified by the NARA-approved Records Schedule in consultation with the Records Management Officer to fulfill the purpose(s) identified in the notice or as required by law;
b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
c. Uses FIPS-validated techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Systems processing, storing, or transmitting PHI:

The organization retains each collection of protected health information (PHI) for a minimum of 6 years from the date of its creation or the date when it was last in effect, whichever is later to fulfill the purpose(s) identified in the notice or as required by law.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Both the Privacy Act and the Federal Records Act require records to be maintained and disposed of in accordance with a published Records Schedule. Disposal and destruction of PII must be done securely so that it may not be reconstructed.
NARA provides retention schedules that govern the disposition of federal records. Program officials and business owners coordinate with records officers, Cyber Risk Advisors, 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 (such as CDs or DVDs), 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.

Reference(s): CFR: 45 C.F.R. §164.310(d)(2)(i), 45 C.F.R. §164.316(b)(2)(i), 45 C.F.R. §164.530(j)(2); Code: 44 U.S.C. Chapter 29, Chapter 31, Chapter 33, 5 U.S.C. §552a(e)(4)(E); E-Gov: §208(e); NIST SP: 800-88; OMB Memo: M-17-12; OMB Circular A-130; Privacy Act: §552a(c)(2), §552a(e)(1)	**Related Controls Requirement(s):** AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The organization retains each collection of PII no longer than the greater of (i) the minimum time period allowable by law, or (ii) the minimum time necessary to fulfill the purpose(s) identified in relevant notices or as required by business needs;
(ii) The organization 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
(iii) The organization uses legally compliant techniques or methods (as defined in NIST SP 800-88 as amended) to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
Determine if:
(i) The system retains PII only if it is pre-determined to be necessary in the authorized data store(s);
(ii) The system has a mechanism for tracking the retention periods associated with the PII it contains;
(iii) The system retains PII no longer than the length of time specified in the applicable Records Control Schedules;
(iv) Backup schedules are designed in accordance with the applicable Records Control Schedules, for systems that handle the backup process;
(v) All instances and formats of each PII data element are locatable and must be deleted when any one instance of that PII is deleted;
(vi) The system supports clean-up of temporary storage it generates in a manner consistent with the retention needs of the system; and
(vii) The system propagates all authorized deletions of PII to target systems in accordance with requirements, for systems that share PII with other systems.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization PII retention policy; PII retention procedures; organization PII disposal policy; PII disposal procedures; other relevant documents or records.
Examine: The system architecture and identify the PII stored by the system.
Examine: Test records processed by the system.
Examine: Interfaces to the data stores to verify that PII is being saved in the intended data stores.
Test: Attempt to use the system to save PII to an unauthorized data store. Comment: Consider the impact of cloud computing, shared disk arrays, and other technologies in identifying the risk of saving information to an incorrect location.
Examine: The data model and data store architecture for retention tracking. Comment: Data tags, date stamps, metadata, and other mechanisms may be used to support this requirement.
Examine: Test data in the system for association with relevant retention periods.
Test: Instantiate test data with a designated retention period and observe what happens when the retention period expires. Comment: Unless there is a business need to retain PII for historical purposes, it should be deleted when no longer needed.
Examine: The backup scripts and procedures to ensure PII is backed up in a manner that is consistent with the retention periods defined in the Records Control Schedules. Comment: Records Control Schedules may vary from system to system. The test assumes that the cognizant authority has approved the Records Control Schedules and that these are consistent with the retention periods documented in the SORN(s) that cover this system. The schedule for rotation and overwriting backup media should be considered to further ensure retention periods are not exceeded.
Examine: Deletion routine for search and delete functionality.
Test: Load test input data to produce multiple instances of processed PII. Initiate processing and deletion, then manually query the database for the presence of each instance of PII.
Examine: The designated locations for temp files created by the system's normal processes. Review the contents of any persistent temp files following a transaction or process involving PII.
Test: Dump the memory contents created by the system's normal processes and review for presence of PII following a transaction or process involving PII. Comment: Heavily system dependent, impacted by operating system, development platform, and specific application code.
Test: Load input test PII into the system. Delete the test PII and confirm that a deletion message was transmitted to applicable target systems. Comment: Deleting downstream PII is not always an appropriate business decision. This test will depend on the documented purposes and requirements of the target systems.

DM-2(1)	System Configuration (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

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 a NARA-approved Records Schedule.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PHI:

HIPAA requires the organization to follow specific procedures for de-identification and to implement policies and procedures to address the final disposition of PHI and/or the hardware or electronic media on which it is stored.

Reference(s): CFR: 45 C.F.R. §164.310(d)(2)(i), 45 C.F.R. §164.514	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

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:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Information system configuration documentation; information system PII audit records; other relevant documents or records. Confirm that information system PII audit records and other relevant documents or records show that information system configures to record the date PII is collected, created or updated and when PII is to be deleted or archived under the approved record retention schedule.

DM-3	Minimization of PII Used in Testing, Training, and Research (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

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.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

When developing and testing information systems, PII is at a heightened risk for accidental loss, theft, or compromise. Therefore, the organization needs to take measures to reduce that risk.

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations 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 Senior Official for Privacy (SOP) and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.

When PII is of a sufficiently sensitive nature, to the greatest extent possible, PII should not be used when testing or developing an information system.

Guidance for Systems processing, storing, or transmitting PHI:

HIPAA has specific requirements for the use of PHI in training or research. As indicated by the HIPAA Privacy Rule's "health care operations" definition (45 C.F.R. §164.501), covered entities may use PHI for conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers. Covered entities may also use PHI for conducting training of non-health care professionals, and in the course of accreditation, certification, licensing, or credentialing activities. For additional information on when and how covered entities may use PHI to conduct research, see 45 C.F.R. §164.512(i).

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:

(i) The organization develops policies and procedures that minimize the use of PII for testing, training, and research; and
(ii) The organization implements controls to protect PII used for testing, training, and research.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

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. Determine whether the organization uses PII for testing or training. If it does, confirm it has documentation describing how the data is protected. Verify the data is protected as described.

DM-3(1)	Risk Minimization Techniques (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Anonymizing PII is one technique to reduce risk and decreases the potential impact if the PII is compromised. Organizations can minimize risk to privacy of PII by using techniques such as de-identification.

When PII is of a sufficiently sensitive nature, to the maximum extent possible, PII should be anonymized in accordance with NIST SP 800-122 prior to its use in development or testing.

Guidance for Systems processing, storing, or transmitting PHI:

Under HIPAA, there are three acceptable approaches to minimizing the risk to privacy when using PHI for research, testing or training. The first is the de-identification of information that results in that information no longer being classified as PHI. There are only two methods for de-identification permitted by HIPAA. For specific details on those two methods see 45 C.F.R. §164.514(a). The second requirement is commonly referred to as the "Minimum Necessary Rule" which limits the amount of PHI used or disclosed to that which is reasonably necessary to accomplish the purpose for which the request for information is made. See 45 §C.F.R. §164.514(d). The third requirement allows covered entities to use or disclose a "limited data set", which excludes certain direct identifiers. Unlike de-identified data, a limited data set is PHI and any use or disclosure must meet specific requirements set out on the HIPAA Privacy Rule. See 45 C.F.R. §164.514(e).

Reference(s):	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

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.

DM-CMS-1	Non-Mandatory: Data Minimization and Retention Control Family Policy and Procedures	Assurance	P3

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A Data Minimization and Retention policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the Data Minimization and Retention policy and associated Data Minimization and Retention controls; and

b. Reviews and updates (as necessary) the current:

1. Data Minimization and Retention policy at least every two (2) years; and

2. Data Minimization and Retention procedures at least every two (2) years.

Implementation Standards:

High & Moderate:

Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the DM family. Policy and procedures reflect applicable federal laws, Executive Orders, 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 program in general and for information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): Code: 44 U.S.C. Chapter 29, Chapter 31, Chapter 33; E-Gov: §208(b), §208(e); NIST SP: 800-88, 800-122; OMB Memo: M-03-22, M-17-12; OMB Circular A-130; Privacy Act: §552a(c)(2), §552a(e), §552a(e)(1)	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Data minimization and retention policy and procedures and other relevant documents.
Interview: Organizational personnel with data minimization and retention responsibilities to ensure responsibilities are acknowledged.

B.23 Individual Participation and Redress (IP)

IP-1	Consent (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:

a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to 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, and retention of PII;
c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Individual participation and agreement to provide information is fundamental to an individual making an informed decision regarding the collection, use, and safeguarding of their PII. Consent is fundamental to the participation of individuals in the decision-making process regarding 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 appropriate notice of the purposes of the PII collection or technology use 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 that 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 act 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 only 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.

Whenever feasible, opt-in is the preferred method to obtain consent.

Guidance for Systems processing, storing, or transmitting PHI:

Consent is a term under HIPAA with specific meaning not equivalent to a HIPAA authorization. For example, see: Uses and disclosures to carry out treatment, payment, or health care operations (45 C.F.R. §164.506); Uses and Disclosures for Which an Authorization is Required (45 C.F.R. §164.508); Uses and Disclosures Requiring an Opportunity to Agree/Object (45 C.F.R. §164.510); Right to Request Privacy Protection for Protected Health Information (45 C.F.R. §164.522).

Reference(s): CFR: 45 C.F.R. §164.506(b), 45 C.F.R. §164.508, 45 C.F.R. §164.510, 45 C.F.R. §164.522; Code: 5 U.S.C. §552a(e)(3)-(4); E-Gov: §208(c); OMB Memo: M-03-22, M-10-22; Privacy Act: §552a(b), §552a(e)(3)	**Related Controls Requirement(s):** 2, AP-1, TR-1, TR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The organization provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;
(ii) 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;
(iii) The organization obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII;
(iv) The organization ensures that 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; and
(v) The user is given the opportunity to provide consent if the system collects PII from that user. Determine if:
(i) The system input interfaces denote specific PII elements that users are required to provide and clearly note that providing all other PII is optional, for systems that collect PII directly from individuals; and
(ii) The system supports a method of tracking consent when appropriate, for systems that collect PII from sources other than the individual.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

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.
Examine: Input screens to verify that user view contains instructions noting the distinction between required and optional PII.
Examine: Input screens to verify that user view clearly marks required data elements.
Examine: Test record for the pre-determined method of tracking/flagging consent. Comment: There are multiple scenarios where this requirement may apply, such as when new PII is created or PII is disclosed in new ways, when legal decisions are made, or when decisions regarding benefits are made. This test will require close coordination with the Business Owner to determine specifics. “Consent” refers to providing individuals the opportunity to give permission regarding how the agency collects, uses, and discloses their PII, including the decision whether to provide PII when practicable. Where consent is relevant, flags or metadata can be used in the record to denote the types of consent allowed and the level of consent provided by the individual.
Test: Create test record with the consent flag enabled and one with the consent flag disabled. Attempt to execute an action that requires use of the consent flag.

IP-1(1)	Mechanisms Supporting Itemized or Tiered Consent (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Individual consent or authorization is required under the HIPAA Privacy Rule for uses and/or disclosures of an individual’s protected health information (PHI). 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.

Guidance for Systems processing, storing, or transmitting PHI:

Individual consent or authorization is required under the HIPAA Privacy Rule for uses and/or disclosures of an individual’s PHI.

Reference(s): CFR: 45 C.F.R. §164.506(b), 45 C.F.R. §164.508	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the system employs a mechanism that supports user-provided consent regarding how their personally identifiable information (PII) is used within the system.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Determine that the system employs a mechanism which support user-provided consent regarding how their PII is used within the system.

IP-2	Individual Access (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:

a. Provides individuals the ability to have access to their PII maintained in its system(s) of records;
b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
c. Publishes access procedures in SORNs; and
d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Implementation Standards:

Systems processing, storing, or transmitting PHI:

PHI.1 - Implement policies and procedures to comply with the regulatory requirements governing an individual's right to access copies of their PHI, including electronic copies.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

The Individual Participation Fair Information Practice Principles (FIPP) requires organizations to provide mechanisms for individuals to gain access to their PII when appropriate. The Privacy Act of 1974, as amended, requires organizations to provide mechanisms for individuals to gain access to their PII when that PII meets the definition of a "record." Access is also an important aspect of supporting correction of PII and redress against alleged violations and misuse of their PII. In addition to access requirements under the Privacy Act of 1974, as amended, HIPAA has statutory requirements to provide access to PHI.
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 Senior Official for Privacy (SOP) working with the Privacy Act Officer 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, however, and heads of agencies may promulgate rules exempting systems from the access provision of the Privacy Act. For example, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding. For other examples where agencies may promulgate rules exempting systems from the access provision, see the Privacy Act at 5 USC § 552a, subsections (j) (General Exemptions) and (k) (Specific Exemptions). Organizations must provide for public access to records, including PII not included in a Privacy Act System of Records, where required or appropriate. While the language of this control is specific to the Privacy Act's requirements for access, FIPPs encourage organizations to use available authorities to provide access when the Privacy Act does not apply. For example, some organizations use the Freedom of Information Act as another tool to provide access to PII for an affected individual.

Reference(s):	**Related Controls Requirement(s):** AR-8, IP-3, TR-1, TR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:

(i) The organization provides individuals the ability to have access to their PII maintained in its system(s) of records;
(ii) The organization publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
(iii) The organization publishes access procedures in SORNs;
(iv) The organization adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests; and
(v) The organization has posted notice to the public for systems that use and collect PII, stating that individuals can access and view their own PII that the system is storing. Determine if:
(i) The system provides immediate notification of the right to and the circumstances under which the individual may access their PII, for systems where individuals directly enter their PII;
(ii) The system enables the individual to review their PII before submitting it for processing, for systems where individuals directly enter their PII; and
(iii) The individual can verify their PII, where authorized, prior to any adverse action being taken based on that PII, for systems that collect PII from a third party.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization policy providing individuals access to their PII maintained in system(s) of records; procedures providing individuals access to their PII maintained in system(s) of record; rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; access procedures in system of records notices (SORN); other relevant documents or records.
Examine: If the system uses and collects PII, confirm they have publicly available documents that allows individuals to access and view their own PII that the system is storing.
Test: Submit test PII to the system and observe any notice provided.
Test: Submit test PII to the system and observe any notice provided. Comment: This requirement applies to all systems that collect PII directly from the individual.
Test: Submit test PII to the system as a third party. Comment: Applies to all systems that collect PII from third parties.
Test: Submit test PII to the system as a third party which produces actionable output. Comment: Applies only to systems that produce actionable output.

IP-3	Redress (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:
a. Provides a process for individuals to have inaccurate, incomplete, or out-of-date PII maintained by the organization corrected or amended, as appropriate; and
b. 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.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Redress supports data integrity requirements for PII by providing a process for individuals to request correction of, or amendment to, their PII maintained by an organization. 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 in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and 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, incomplete, or out-of-date 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.

Reference(s): CFR: 45 C.F.R. §164.526; Code: 5 U.S.C. §552a(c)(4), (d), and (h); OMB Circular A-130; Privacy Act: §552a(c)(4), §552a(d)	**Related Controls Requirement(s):** IP-2, TR-1, TR-2, UL-2, DI- 1

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The organization provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate;
(ii) 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; and
(iii) The redress policy and procedures allow an individual to make corrections to any information about that individual. Determine if:
(i) The system notifies the individual either directly or indirectly of adverse output based on PII submitted to the system and notify the individual of the mechanisms for redress;
(ii) The system notifies the third parties of the mechanisms and circumstances governing the update/ correction of the submitted PII, for systems that receive PII from third parties;
(iii) The system enables the organization to update/correct submitted PII, for systems that receive PII from third parties;
(iv) The system enables the organization to update/correct the submitted PII, for systems that receive PII from source systems;
(v) The system provides immediate notification of the right to and the circumstances under which the individual may update/correct their PII, for systems into which individuals directly enter their PII;
(vi) The system maintains a flag indicating that the PII is in dispute, when the individual disputes the accuracy of PII or any output based on the disputed PII; and
(vii) the system propagates all authorized updates/corrections of PII to target systems.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Redress process policy and procedure.
Test: Submit test PII that results in adverse output. Comment: This requirement applies to systems that may produce adverse actionable output based on PII.
Test: Submit test PII as a third party to the system and observe any notice provided. Comment: This requirement applies to all systems that collect, process, or transmit PII. **Test:** Submit test PII to the system as a third party, then attempt to update the test PII originally submitted. Comment: This requirement applies to all systems that collect, process, or transmit PII.
Test: Submit test PII to the system from a source system, then attempt to update the test PII originally submitted. Comment: This requirement applies to all systems that collect, process, or transmit PII.
Test: Enter test PII into the system and observe any notice provided. Comment: This requirement applies to all systems that collect, process, or transmit PII.
Test: Submit test PII to the system. Subsequently submit a dispute of the same PII. Comment: This requirement applies to systems that may produce adverse actionable output based on PII.
Test: Submit updated test PII to the system and verify that the update is transmitted to target systems.

IP-4	Complaint Management (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Establishing a complaint management process ensures complaints are addressed in a timely manner and provides an avenue for individuals to participate in government activities that may impact privacy. Information received from complaints provides external input regarding organizational privacy and security practices which may improve processes and systems involved in collection, use, and maintenance of personally identifiable information (PII).
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 (including contact information for the Senior Official for Privacy (SOP) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.

Reference(s): CFR: 45 C.F.R. §164.530 (d); OMB Memo: M-17-12, M-08-09; OMB Circular A-130: 7.g.	**Related Controls Requirement(s):** AR-6, IP-3

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if there are adequate procedures for handling privacy related inquiries and complaints.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Procedural documents for handling privacy related inquiries and complaints.
Interview: The ISSO and/or Data Guardian and request a list of personnel who is responsible for managing the complaints.
Examine: Sample inquiries and complaints.

IP-4(1)	Response Times (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:
a. Acknowledges complaints, concerns, or questions from individuals within ten (10) working days;
b. Completes review of requests within thirty (30) working days of receipt, unless unusual or exceptional circumstances preclude completing action by that time; and
c. Responds to any appeal as soon as possible, but no later than thirty (30) working days after receipt of the appeal unless the appeal authority can show good cause to extend the response period.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Timely communication and resolution of complaints from individuals demonstrates responsiveness by the organization and reduces the organization's risk of reputational damage and potential lawsuits under HIPAA.
Timely communication and resolution of complaints from individuals demonstrates responsiveness by the organization and reduces the organization's risk of reputational damage and potential lawsuits under the Privacy Act. Organizations should establish a complaint management process that ensures complaints are resolved within a reasonable amount of time.

Reference(s): CFR: 45 C.F.R. §164.520(b)(1)(vi); Code: 5 U.S.C. §552a; OMB Circular A-130: 7.g.	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the organization responds to complaints, concerns, or questions from individuals within the CMS-defined time period.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Process for responding to complaints, concerns, or questions from individuals; other relevant documents or records.

IP-CMS-1	Non-Mandatory: Individual Participation and Redress Control Family Policy and Procedures	Assurance	P3

Control:

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. Individual Participation and Redress policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the Individual Participation and Redress policy and associated Individual Participation and Redress controls; and
b. Reviews and updates (as necessary) the current:
1. Individual Participation and Redress policy at least every two (2) years; and
2. Individual Participation and Redress procedures at least every two (2) years.

Implementation Standards:

High & Moderate:

Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IP family. Policy and procedures reflect applicable federal laws, Executive Orders, 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 program in general and for information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): E-Gov: §208(c); OMB Memo: M-03-22, M-17-12, M-08-09, M-10-22; OMB Circular A-130; Privacy Act: §552a(b), §552a(c)(3), §552a(c)(4), §552a(d), §552a(d)(5), §552a(e)(3), §552a(e)(4), §552a(j), §552a(k), §552a(t)	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Individual participation and redress policy and procedures, and other relevant documents.
Interview: Organizational personnel with individual participation and redress responsibilities to ensure responsibilities are acknowledged.

B.24 Security (SE)

SE-1	Inventory of Personally Identifiable Information (High, Moderate, Low)	P1

Control:

The organization:

a. Establishes, maintains, and updates, no less often than once 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 PII; and

b. Provides each update of the PII inventory to the CMS Senior Official for Privacy (SOP) and the CMS CISO no less often than once every three hundred sixty-five 365 days to support the establishment of information security requirements for all new or modified information systems containing PII.

Supplemental Guidance:

The PII inventory identifies the organization's information assets and identifies those assets collecting, using, maintaining, or sharing PII. The PII inventory identifies those assets most likely to impact privacy; provides a starting point for organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII; and to mitigate risks of PII exposure.

The PII inventory enables organizations to identify systems and programs that contain PII so that they can then identify and address privacy risks. 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. Organizations gather information on the location of PII as they are developing and updating systems and programs. In addition, they cross reference information in privacy impact assessments (PIA) and system of records notices (SORN) to ensure that PIAs and SORNs are consistent with the PII inventory. Organizations may extract the following information elements from Privacy Impact Assessments (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 creating and updating the inventories by identifying linkable data that could create PII.

Reference(s): CFR: 45 C.F.R. §164.530(c); 45 C.F.R. §164.310(d); Code: 5 U.S.C. §552a(e)(10); Pub. L. No. 107-347, §208(b)(2); E-Gov: §208(b)(2); FIPS Pub: 199; NIST SP: 800-37, 800-122; OMB Memo: M-03-22, M-17-12 Att. 1, B.1.a, M-16-04; OMB Circular A-130: Appendix I; Privacy Act: §552a(e)(10)	**Related Controls Requirement(s):** AR-1, AR-4, AR-5, AT-1, CM-8, DM-1, PM-5

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if:

(i) The organization establishes, maintains, and updates, no less often than once 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 PII;

(ii) The organization provides each update of the PII inventory to the SOP and the CISO to support the establishment of information security requirements for all new or modified information systems containing PII; and

(iii) The inventory list of all systems that are collecting and maintaining PII are accurate and complete.

Assessment Methods and Objects:

Examine: Request and review the inventory list of all systems that are collecting and maintaining PII.

SE-2	Privacy Incident Response (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:

a. Develops and implements a Privacy Incident and Breach Response Plan; and

b. Provides an organized and effective response to privacy incidents and breaches in accordance with HHS and CMS Privacy Incident (and Breach) Response Plans.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Developing and implementing a risk-based analysis for privacy breaches using a "Best Judgment Standard" as described in this control's supplemental guidance ensures consistency in, and avoids over-reporting of, privacy breach notifications.

The organizational Privacy Incident and Breach Response Plan may be integrated with the organizational Incident Response Plan. The organization privacy incident and breach response capability must be able to demonstrate knowledge of the privacy incident and breach response processes and procedures and evidence showing the plan is followed routinely while responding to privacy incidents and breaches.

In contrast to the Incident Response (IR) family in NIST 800-53 Appendix F, 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 personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the Senior Official for Privacy (SOP). The plan includes:

(i) The establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan;

(ii) A process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly;

(iii) 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;

(iv) Internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to the SOP and other designated officials consistent with organizational incident management structures; and

(v) Internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach.

Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans or keep the plans separate.

The Best Judgment Standard, explained in OMB M-17-12, Footnote 6, imposes a requirement for organizations to develop and implement a risk-based analysis for privacy breaches to determine whether the breach needs to be reported. The Best Judgment Standard gives organizations responsibility for their own data in two important ways. First, the organization must determine the sensitivity of its PII, based on the information and the context in which the information appears. Second, the organization must determine whether a privacy breach should be reported, based on the resultant privacy risk to the organization and to affected individuals. The Best Judgment Standard effectively imposes a requirement on organizations to develop and implement a risk-based analysis for privacy breaches to determine whether the breach needs to be reported. In the context of breach reporting, the purpose of the Best Judgment Standard is to limit reporting to those privacy breaches which meet the organization's risk threshold.

Conversely, under the Best Judgment Standard, organizations are not required to report privacy breaches that do not meet their risk threshold. The policy provides an example of implementing the Best Judgment Standard as discarding a document with the author's name on the front and no other PII into an office trashcan, positing that this probably would fall below and organization's risk threshold and would not need to be reported.

OMB M-17-12 does not provide bright line rules to define what is considered "sensitive PII" using the common dictionary definition approach to the language in the memorandum–and under what circumstances a privacy breach should be reported, both because it would be a futile effort to attempt to delineate or predict the myriad potential contexts and situations, and agencies are in the best position to know and understand the relevant circumstances of their PII to determine which PII is sensitive and which breaches create risk.

Reference(s): CFR: 45 C.F.R. Part 164 Subpart D; 45 C.F.R. §164.308(a)(6); NIST SP: 800-37; OMB Memo: M-06-19, M-17-12; Privacy Act: §552a(e), §552a(i)(1), §552a(m)	**Related Controls Requirement(s):** AR-1, AR-4, AR-5, AR-6, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-13, AU-14, IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, RA-1

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The organization develops and implements a Privacy Incident and Breach Response Plan; and
(ii) The organization provides an organized and effective response to privacy incidents and breaches in accordance with HHS and CMS Privacy Incident (and Breach) Response Plans.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization Privacy Incident Response Plan; privacy incident response procedures; other relevant documents or records.
Interview: Organizational personnel with privacy incident and breach response planning responsibilities.
Test: Organizational privacy incident and breach response plan and related organizational processes.
Examine: Review the Privacy Incident Response Plan or verify a privacy section is present with the ISRA and accurately reflect CMSR v. 2.0 guidelines.

SE-CMS-1	Non-Mandatory: Security Control Family Policy and Procedures	P3

Control:

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. Security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the Security policy and associated Security controls; and
b. Reviews and updates (as necessary) the current:
1. Security policy at least every two (2) years; and
2. Security procedures at least every two (2) years.

Implementation Standards:

High & Moderate:

Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SE family. Policy and procedures reflect applicable federal laws, Executive Orders, 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 program in general and for information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): E-Gov: §208(b)(2); FIPS Pub: 199; NIST SP: 800-37, 800-122; OMB Memo: M-06-19, M-17-12, M-03-22, M-16-04; OMB Circular A-130: Appendix I; Privacy Act: §552a(e), §552a(e)(10), §552a(i)(1), §552a(m)	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Privacy's security policy and procedures, and other relevant documents.
Interview: Organizational personnel with privacy's security responsibilities to ensure responsibilities are acknowledged.

B.25 Transparency (TR)

TR-1	Privacy Notice (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:

a. Provides effective notice to the public and to individuals regarding:
(i) Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;
(ii) Authority for collecting PII;
(iii) The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and
(iv) The ability to access and have PII amended or corrected if necessary.
b. Describes:
(i) The PII the organization collects and the purpose(s) for which it collects that information;
(ii) How the organization uses PII internally;
(iii) Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;
(iv) Whether individuals can consent to specific uses or sharing of PII and how to exercise any such consent;
(v) How individuals may obtain access to PII; and
(vi) 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.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Providing the appropriate notification of privacy practices to the individual enables the individual to make an informed decision when they provide their consent. 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 that the organization has addressed in implementing its information practices. The organization may provide public notice through a variety of means. Some of these may be required by law or regulations, such as system of records notices (SORN) for Privacy Act systems, privacy impact assessments (PIA) for agency information systems and electronic collections of information, and website privacy policies for agency websites. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The Senior Official for Privacy (SOP) is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control may be satisfied by an organization's compliance with the public notice requirements of federal laws, regulations, and guidelines, such as:

- Provisions of the Privacy Act,
- The E-Government Act's PIA requirement,
- OMB Memoranda including M 03-22 (*Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*), 17-06 (*Policies for Federal Agency Public Websites and Digital Services*), 10-22 (*Guidance for Online Use of Web Measurement and Customization Technology*), and 10-23 (*Guidance for Agency Use of Third-Party Websites and Applications*),
- The Children's Online Privacy Protection Act (COPPA), and
- The HIPAA Privacy Rule, Section 45 CFR § 164.520, "Notice of privacy practices for protected health information."

Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SOP and Chief Counsel.

The website privacy policy described by OMB M-17-12, *Policies for Federal Agency Public Websites and Digital Services*, frequently referred to on organization websites as a "Privacy Policy" or "Privacy and Security Notice," is intended as a broad notice of website privacy policies and general website use, and will not by itself meet the requirement for specific notice when collecting PII. When PII is maintained (including collection) in a system of records that is covered by the Privacy Act, the organization must provide a "Privacy Act Statement" to the individual at the time of collection that meets the requirements of the Privacy Act of 1974, 5 U.S.C. §552a(e)(3), unless the organization has published a rule exempting that system of records from the (e)(3) notice provision in accordance with subsection (j) of the Privacy Act. If the PII is not maintained in a system of records under the Privacy Act, a privacy notice should be provided which describes the privacy practices associated with that PII, including, but not limited to, the way the PII is protected, how it is used, and whether it is shared. To avoid confusion, this type of privacy notice must not be labeled as a "Privacy Act Statement." As an alternative, several organizations refer to this notice type as a "Privacy Advisory."

Guidance for Systems processing, storing, or transmitting PHI:

The HIPAA Privacy Rule also requires a privacy notice referred to as a "Notice of Privacy Practices." For specific rules on this notice please refer to 45 C.F.R. §164.520.

Reference(s):	Related Controls Requirement(s): AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:

(i) The organization provides effective notice to the public and to individuals regarding their privacy program policies and practices that includes:
- 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.

(ii) 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 of such sharing;
- Whether individuals can 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.

(iii) 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.

Determine if privacy notices are accurate and complete for systems that collect PII.

Determine if the system provides notice of the privacy practices associated with the system, the PII collected, and a description of how the PII is used and managed, for systems that collect PII directly from individuals.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Public notice regarding individual privacy and PII; other relevant documents or records.

Examine: If the system collects PII, confirm it has a privacy notice that describes:

(i) The PII the organization collects and the purpose(s) for which it collects that information;

(ii) How the organization uses PII internally;

(iii) Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;

(iv) Whether individuals can consent to specific uses or sharing of PII and how to exercise any such consent;

(v) How individuals may obtain access to PII; and

(vi) How the PII will be protected.

Test: Attempt to enter test PII as an individual using the system. Observe any notice provided by the system. Comment: Notice at the point of collecting PII directly from the individual allows for the assumption that the individual is providing consent for the PII collected and the purposes for which it will be used. There are various methods of providing notices through systems, depending on the purposes of the system. For example, notice may be provided through the website privacy policy, as a pop-up box, end-user agreement, or as text located above the input fields for PII.

TR-1(1)	Real-Time or Layered Notice (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization provides real-time and/or layered notice when it collects PII.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Real-time notice facilitates informed consent and promotes trust from the individual when collecting sensitive PII. Real-time notice used in conjunction with a Privacy Act Statement or Privacy Advisory, based on the sensitivity of the PII provided or collected, ensures the individual provides informed consent.
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/specific information.

Guidance for Systems processing, storing, or transmitting PHI:

The HIPAA Privacy Rule provides the option of layered notice to allow for simplified up-front notification with greater detail following. The Department of Health and Human Services has provided both guidance and model notices of privacy practices (see http://www.hh.gov/ocr/privacy/hipaa/modelnotices.html for details).

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if a privacy notice is placed at the point of collections for systems that collect PII.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: If the system collects PII, verify a privacy notice is placed at the point of collection.

TR-2	System of Records Notices and Privacy Act Statements (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization, through the HHS Privacy Act Officer, OpDiv Privacy Contacts, and the HHS Office of General Counsel:
a. Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII that are subject to the Privacy Act;
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.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

SORNs and Privacy Act Statements, i.e., (e)(3) notices, provide transparency, in advance of collection, use, maintenance, or sharing of PII when in a system that meets the statutory definition of a "system of records" under the Privacy Act. The Privacy Act notes that it uses "maintain" to include "maintain, collect, use or disseminate." These requirements impact decisions made during planning, design, development, and operation of programs and systems.
Organizations issue 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 another 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. Privacy Act Statements provide notice of:
(i) the authority of organizations to collect PII;
(ii) whether providing PII is mandatory or optional;
(iii) the principal purpose(s) for which the PII is to be used;
(iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information 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).
The Privacy Act and OMB guidance set forth specific requirements regarding when and how notices are provided. In addition to any internal organization review process, the publication of a SORN in the Federal Register requires a mandatory review and comment period of a minimum of 40 days.
Regarding TR-2, paragraph a, the publication of a SORN is required only when the PII is maintained in a system that meets the statutory definition of a "system of records" under the Privacy Act. Not all systems containing PII may meet the definition of a "system of records." However, all PII maintained by an organization must be protected irrespective of whether the PII is subject to the Privacy Act.
Regarding TR-2, paragraph c, the Privacy Act Statement, when required, should be provided in the same format as the information is collected. For example, an electronic statement on a website, a written statement on a paper form, and a verbal statement provided for information that is collected verbally.

Reference(s): Code: 5 U.S.C. §552a(e)(3)-(e)(4); OMB Circular A-130; Privacy Act: §552a(e)(3)	**Related Controls Requirement(s):** DI-2

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the system has a SORN in the Federal Register.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Verify the system has a SORN in the Federal Register.

TR-2(1)	Public Website Publication (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization publishes SORNs on its public website.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - SORNs must be published on the CMS systems of records website at http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and- Systems/Privacy/CMS-Systems-of-Records.html

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Publishing SORNs on organization websites improves transparency by providing individuals easier access to information about how their PII will be collected, used, maintained, or shared; and centralizing the information regarding to whom an individual should submit a request for access or amendment to their information covered by the SORN.
The organization may establish a centralized website for publication of their SORNs.

Reference(s): Code: 5 U.S.C. §552a(e)(4;); OMB Circular A-130: 7.g. and Appendix I	Related Controls Requirement(s):

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if the current SORN is located on the CMS dedicated website.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Verify that the current SORN is located on http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/CMS-Systems-of-Records.html

TR-3	Dissemination of Privacy Program Information (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:

a. Ensures that the public has access to information about its privacy activities and can communicate with its Senior Official for Privacy (SOP); and
b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Making information about an organization's privacy program readily available to the public reduces the burden on individuals wanting to better understand an organization's privacy practices; and reduces burden on privacy offices and program officials by providing answers to common privacy questions through an easily accessible forum. Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, privacy impact assessments (PIA), system of records notices (SORN), 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.

Reference(s): Code: 5 U.S.C. §552a(e)(4); Pub. L. No. 107-347, §208(b)(1)(B)(iii); E-Gov: §208; OMB Memo: M-03-22, M-10-23 Section 4 Privacy Act: §552a	Related Controls Requirement(s): AR-6

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if information regarding privacy policies are publicly available.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Verify information regarding privacy policies are publicly available. For example, HHS and CMS maintains program specific privacy policies and documentation at the following websites:
CMS Privacy Program Page - https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/index.html. HHS Privacy Impact Assessment Page - http://www.hhs.gov/pia/
Information Security and Privacy Library - https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information- Security-Library.html

TR-CMS-1	Non-Mandatory: Transparency Control Family Policy and Procedures	Assurance	P3

Control:

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. Transparency policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the Transparency policy and associated Transparency controls.
b. Reviews and updates (as necessary) the current:
1. Transparency policy at least every two (2) years; and
2. Transparency procedures at least every two (2) years.

Implementation Standards:

High & Moderate:

Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the TR family. Policy and procedures reflect applicable federal laws, Executive Orders, 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 program in general and for information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Reference(s): E-Gov: §208(b); OMB Memo: M-03-22, M-17-12, M-10-22, M-10-23; OMB Circular A-130; Privacy Act: §552a, §552a(e)(3), §552a(e)(4)	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Transparency policy and procedures, and other relevant documents.
Interview: Organizational personnel with transparency responsibilities to ensure responsibilities are acknowledged.

B.26 Use Limitation (UL)

UL-1	Internal Use (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - All PII must be used for an official government purpose only. The officers and employees of the organization must have a need for the PII in the performance of their official duties. These requirements apply to all PII regardless of its coverage by the Privacy Act.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Consistent with the Privacy Act, the organization's internal use of PII contained in a system of records notice (SORN) is limited to the purposes identified in one of the 12 exceptions to Section b of the Privacy Act and as described in the SORN. Consistent with the Fair Information Practice Principles (FIPP) and Section 208 of the E- Government Act, the organization's internal use of PII not contained in a SORN should be compatible with the purpose for which it was originally collected and as described in the PIA or other public notice. Organizations take steps to ensure that 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 Senior Official for Privacy (SOP) 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.
The phrase "authorization schema" refers to the logic of how authorization permissions are designed to function within the system (e.g., by group, by role, by transaction type, etc.). An example of an authorization schema where permissions appropriately match functions would be a schema where a group of "reviewers" is separate from a group of "approvers." Individuals assigned to the "reviewer" group could read PII and make recommendations, but not approve actions. Individuals in the "approver" group could read recommendations and approve actions. An authorization schema where all individuals are automatically authorized to approve all actions is an example of a schema where the alignment between permissions and functions may be inappropriate.

Reference(s): CFR: 45 C.F.R. §164.502; 45 C.F.R. §164.504; 45 C.F.R. §164.506; 45 C.F.R. §164.508; 45 C.F.R. §164.510; 45 C.F.R. §164.512; 45 C.F.R. §164.514 Code: 5 U.S.C. §552a; Pub. L. No. 107-347, §208; OMB Circular A-130: 7.g.; Privacy Act: §552a(b)(1)	**Related Controls Requirement(s):** AC-2, AC-3, AC-5, AC-6, AC-8, AC-21, AU-2, AU-3, AU-10, AU-14, IA-2, PS-1, PS-2, PS-3, AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices Determine if:
(i) The system's use of PII is consistent with the privacy notices related to the system, including any SORN, Privacy Impact Assessment, and/or notices provided at points of collection;
(ii) The system's disclosures of PII are consistent with the privacy notices related to the system, including any SORN, Privacy Impact Assessment, and/or notices provided at points of collection;
(iii) The authorization schema for the system aligns with the business logic within the system;
(iv) The system responds to authorization changes within a defined timeframe;
(v) The system connects to source systems to process changes in authorizations based on relevant organizational events (e.g., separations, job changes, etc.); and
(vi) The system requests appropriate credentials at the time of request for initial access to sufficiently identify the user/system making the request.

Assessment Methods and Objects:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization privacy policy; organization privacy practices; other relevant documents or records.
Examine: Documented system functions with relevant privacy notices.
Examine: Documented system outputs with relevant privacy notices.
Examine: The functions of the system and the authorization schema of the system, and compare them for alignment. Comment: If the authorization schema is not in alignment with business functions it could result in entities having greater access to PII than needed.
Examine: The authorization schema and compare it to the SORN and any applicable Computer Matching Agreements and data sharing memoranda of understanding (MOU)/memoranda of agreement (MOA). Comment: If the authorization schema allows for access or roles that are not included as part of relevant privacy documents, the system will be in violation of the Privacy Act of 1974.
Examine: A sample of the existing or proposed users/systems and compare their business responsibilities to their permissions within the system. Comment: If the authorization schema is too broad, it will result in entities having greater access to PII than needed; if the schema is too narrow, it will result in overly burdensome administration of the system authorizations.
Test: Remove a user/system's authorization to access the system.
Test: Remove a user/system's authorization permission.
Test: Reduce the authorization status of a user/system.
Examine: The system design to verify that the system connects to all the appropriate source systems for changes in user/system status.
Test: Make a change to a user/system's status in the source system such that access to the system being tested would be removed or reduced (e.g., a separation). **Test:** Make a change to a user/system's status in the source system such that a specific permission authority would be removed (e.g., a department change). Comment: The number of test cases may vary based on:
(1) The PII and processing capabilities of the system;
(2) The technology platform of the system; and
(3) Connections to any centralized authorization facilities.
Test: Attempt to gain access to the system without entering appropriate credentials.
Test: Attempt to gain access to the system with valid credentials.
Test: Attempt to gain access to the system as multiple users/systems.

UL-2	Information Sharing with Third Parties (High, Moderate, Low)	P1

Control:

Systems processing, storing, or transmitting PII (to include PHI):

The organization:

a. 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;
b. Where appropriate, enters into MOUs, MOAs, 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;
c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Implementation Standards:

Systems processing, storing, or transmitting PII (to include PHI):

High & Moderate:

PRIV.1 - Consistent with the Purpose Specification and Use Limitation Fair Information Practice Principles (FIPPs), sharing of PII must be compatible with the purpose for which it was collected. Consistent with the Transparency FIPP, any subsequent sharing that is not compatible may not be done until additional notice is provided to the individual, their consent is obtained, and relevant documents are updated or published; e.g., when applicable and appropriate, publish an updated system of records notice (SORN) to cover the additional incompatible sharing and obtain consent from the affected individuals.

Supplemental Guidance:

Guidance for Systems processing, storing, or transmitting PII (to include PHI):

Sharing PII with third parties introduces new risks to the individual which, as applicable, requires organizations to establish formal agreements with the third party and to ensure the sharing is compatible with the purposes described in any notice to, and consent from, the individual. Consideration of privacy risks for sharing PII apply regardless of the method used or whether the information remains stored in the system of records. Data removed from an information system covered by a system of records notice (e.g., a Human Resources [HR] database) and shared in another format (e.g., an Excel spreadsheet) must still meet purpose and use requirements of the associated notice. PII not in a system of records that is shared with a third party still must meet the Purpose Specification and, relatedly, Use Limitation FIPPs. For example, data extracts of PII shared via an Excel spreadsheet or database archive must still be shared only if consistent with purposes set out in notices provided to the individual, and in any consent or authorization received from that individual.
A "third party" for these purposes is an individual or organization other than CMS and the individual about whom CMS collects and uses information.
The organization SOP 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 privacy impact assessment (PIA), SORN, 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.

Guidance for Systems processing, storing, or transmitting PHI:

Under HIPAA Privacy Rule, a covered entity may not use, disclose or request a medical record, except when the medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. The disclosure and sharing of PHI is governed by the HIPAA regulations. For details consult the HIPAA Privacy and Security rules at: http://www.hhs.gov/ocr/privacy/index.html.

Reference(s): CFR: 45 C.F.R. §164.502(e)(1), 45 C.F.R. §164.514(e)(1); Code: 5 U.S.C. §552a; Guide: Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment; Privacy Act: §552a(a)(7), §552a(b), §552a(c), §552a(e)(3)(C), §552a(o)	**Related Controls Requirement(s):** AP-2, AR-3, AR-4, AR-5, AR-8, DI-1, DI-2, IP-1, TR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Systems processing, storing, or transmitting PII (to include PHI):

Determine if:
(i) 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;

(ii) The organization where appropriate, enters into MOUs, MOAs, 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;
(iii) 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
(iv) 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:

Systems processing, storing, or transmitting PII (to include PHI):

Examine: Organization privacy policy; organization privacy practices; MOUs, MOAs, Letters of Intent, CMAs, or similar agreements with third parties; system configuration; audit records; training records; and other relevant documents or records.

UL-CMS-1	Non-Mandatory: Use Limitation Control Family Policy and Procedures	Assurance	P3

Control:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A Use Limitation policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the Use Limitation policy and associated Use Limitation controls; and

b. Reviews and updates (as necessary) the current:

1. Use Limitation policy at least every two (2) years; and
2. Use Limitation procedures at least every two (2) years.

Implementation Standards:

High & Moderate:

Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the UL family.

Reference(s): Privacy Act: §552a(a)(7), §552a(b), §552a(b)(1), §552a(c), §552a(e)(3)(C), §552a(o)	**Related Controls Requirement(s):** AR-1

ASSESSMENT PROCEDURE

Assessment Objective:

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

Assessment Methods and Objects:

Examine: Use limitation policy and procedures, and other relevant documents.
Interview: Organizational personnel with use limitation responsibilities to ensure responsibilities are acknowledged.

Appendix C. Acronyms

Acronym	Definition
ABAC	Attribute-Based Access Control
AC	Access Control
ACL	Access Control List
AO	Authorizing Official
AP	Authority and Purpose
API	Application Programming Interface
APT	Advanced Persistent Threat
AR	Accountability, Audit, and Risk Management
ARS	Acceptable Risk Safeguards
AT	Awareness and Training
ATO	Authority to Operate
AU	Audit and Accountability
BCP	Business Continuity Plan
BDC	Baltimore Data Center
BIOS	Basic Input Output System
BYOD	Bring Your Own Device
C.F.R.	Code of Federal Regulations
CA	Security Assessment and Authorization
CAC	Common Access Card
CCB	Change Control Board
CCIC	CMS Cybersecurity Integration Center
CERT	Computer Emergency Response Team
CFACTS	CMS FISMA Controls Tracking System
CFE	Contractor Furnished Equipment
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMA	Computer Matching Agreement

Acronym	Definition
CMS	Centers for Medicare & Medicaid Services
CMSR	CMS Minimum Security Requirements
CNSS	Committee for National Security Systems
CO	Contracting Officer
COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf
CP	Contingency Planning
CPC	Contingency Plan Coordinator
CPO	Chief Privacy Officer
CRA	Cyber Risk Advisor
CRL	Certificate Revocation List
CRO	Chief Risk Officer
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CybOX	Cyber Observable eXpression
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DI	Data Quality and Integrity
DIB	Data Integrity Board
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DM	Data Minimization and Retention
DMZ	Demilitarized Zone
DNS	Domain Name Service
DNSSEC	DNS Security
DoB	Date of Birth

Acronym	Definition
DoD	Department of Defense
DRP	Disaster Recovery Plan
EAP/TLS	Extensible Authentication Protocol/Transport Layer Security
EPLC	Enterprise Performance Lifecycle
ERA	E-Authentication Risk Assessment
FAR	Federal Acquisition Regulation
FEA	Federal Enterprise Architecture
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential and Access Management
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standard
FISCAM	Federal Information Systems Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
FTI	Federal Tax Information
FTP	File Transfer Protocol
GAO	Government Accountability Office
GFE	Government Furnished Information
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HR	Human Resources
HSPD	Homeland Security Presidential Directive
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
IA	Identification and Authentication
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IOC	Indicators of Compromise
IP	Individual Participation and Redress

Acronym	Definition
IP	Internet Protocol
IPS	Intrusion Protection System
IR	Incident Response
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS	Information System
IS2P	Information Systems Security and Privacy
IS2P2	Information Systems Security and Privacy Policy
ISA	Information Sharing Agreement
ISAC	Information Sharing and Analysis Center
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISE	Information Sharing Environment
ISO	International Organization for Standardization
ISPG	Information Security and Privacy Group
ISRA	Information Security Risk Assessment
ISSO	Information System Security Officer
IT	Information Technology
JAB	Joint Authorization Board
LACS	Logical Access Control System
MA	Maintenance
MAC	Mandatory Access Control
MDCN	Medicare Data Communications Network
MFA	Multifactor Authentication
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
MPLS	Multi-Protocol Label Switching
MTD	Maximum Tolerable Downtime
NAC	Network Access Control
NARA	National Archives and Records Administration
NCP	National Checklist Program
NIAP	National Information Assurance Partnership

Acronym	Definition
NIST	National Institute of Standards and Technology
NOFORN	Not Releasable to Foreign Nationals
NSA	National Security Agency
NSS	National Security System
NTP	Network Time Protocol
NVD	National Vulnerability Database
OCISO	Office of the Chief Information Security Officer
OCSP	Online Certificate Status Protocol
OEP	Occupant Emergency Plan
OIT	Office of Information Technology
OMB	Office of Management and Budget
OpDiv	Operating Division
OPM	Office of Personnel Management
OS	Operating System
OVAL	Open Vulnerability Assessment Language
P0	Priority Code 0 (not selected)
P1	Priority Code 1 (Highest)
P2	Priority Code 2
P3	Priority Code 3 (Lowest)
PaaS	Platform as a Service
PACS	Physical Access Control System
PAS	Privacy Act Statement
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PEAP	Protected Extensible Authentication Protocol
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning
PL	Public Law

Acronym	Definition
PM	Program Management
PMEF	Primary Mission Essential Function
POA&M	Plan of Action and Milestones
PS	Personnel Security
RA	Risk Assessment
RBAC	Role-Based Access Control
RBT	Role-Based Training
RDP	Remote Desktop Protocol
RMH	Risk Management Handbook
RoB	Rules of Behavior
RTO	Recovery Time Objective
SA	System Acquisition
SA&A	Security Assessment and Authorization
SAOP	Senior Agency Official for Privacy
SC	System and Communications Protection
SCA	Security Control Assessment
SCAP	Security Content Automation Protocol
SDLC	System Development Life Cycle
SE	Security
SFTP	Secure File Transfer Protocol
SI	System and Information Integrity
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SNMP	Secure Network Management Protocol
SOC	Security Operations Center
SOP	Senior Official for Privacy
SORN	System of Records Notice
SP	Special Publication
SSH	Secure Shell
SSN	Social Security Number
SSP	System Security Plan
STIG	Security Technical Implementation Guide
STIX	Structured Threat Information eXpression

Acronym	Definition
TAXII	Trusted Automated eXchange of Indicator Information
TCP	Transmission Control Protocol
TIC	Trusted Internet Connection
TR	Transparency
TRA	Technical Reference Architecture
TRB	Technical Review Board
UL	Use Limitation
U.S.C.	United States Code
URL	Universal Resource Locator
USB	Universal Series Bus
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
UTC	Continued Universal Time
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WLAN	Wireless Local Area Network
WORM	Write Once Read Many
XLC	eXpedited Life Cycle

This page intentionally blank.

Appendix D. Glossary

Term	Definition
CMS Sensitive Information	*CMS Sensitive Information* is defined in the RMH Volume I Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms*. CMS Sensitive Information is subject to Executive Order 13556, *Controlled Unclassified Information*. This definition includes all data that require protection due to the risk and magnitude of loss or harm, such as Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI).
Control	A security or privacy *Control* is the concise statement specifying specific activities or actions needed to protect an aspect of the CMS information or information system at the applicable system security level. Controls are mandatory when defined under the CMSR baseline associated with each FIPS 199 security categorization. However, security or privacy controls may be selected by the Business Owner to strengthen the level of protection provided if deemed appropriate to mitigate or reduce risk.
Control Baseline	A *Control Baseline* is the minimum list of security and privacy controls required for safeguarding an IT system based on the organizationally identified needs for confidentiality, integrity, and/or availability. A different baseline exists for each security category.
Control Enhancement	*Control Enhancements* supplement controls to achieve the overall required level of protection in accordance with the system security level. Control enhancements are mandatory when defined under the CMSR baseline associated with each FIPS 199 security categorization. However, control enhancements may be selected by the Business Owner to strengthen the level of protection provided if deemed appropriate to mitigate or reduce risk.
External Requirements	*External Requirements* are requirements from authorities, both internal and external to CMS, that are imposed on at least some information systems and business processes. It is the responsibility of the Business Owners of CMS systems, with direction provided by the Office of Information Technology (OIT), to ensure that all applicable internal/external information security and privacy assurance controls are incorporated into CMS systems.
Implementation Standard	An *Implementation Standard* is associated with a security or privacy control or control enhancement. The purpose of the implementation standard is to provide a common standard for implementation across CMS for the associated control or control enhancement.

Term	Definition
Mandatory Control and Control Enhancement	*Mandatory Controls and Control Enhancements* have been selected by for one or more of the FIPS 199 security category-based baselines defined by CMS. *Mandatory Controls and Control Enhancements*, collectively known as the CMS Minimal Security Requirement (CMSR) baselines, are required to meet CMS mission and business requirements *Mandatory Controls and Enhancements* must be documented within applicable security plans/information security risk assessment.
Non-Mandatory Control and Control Enhancement	*Non-Mandatory Controls and Control Enhancements* have not been selected under one or more of the FIPS 199 security category-based baselines defined by CMS. However, *Non-Mandatory Controls and Control Enhancements* may offer additional protection that should be considered by the Business Owner as part of risk-based decision/risk management process. *Non-Mandatory Controls and Control Enhancements* apply to all FIPS 199 security categories. Implemented *Non-Mandatory Controls and Control Enhancements* must be documented within applicable security plans/information security risk assessment.
Residual Risk	*Residual Risk* is the risk remaining after efforts have been made to mitigate or eliminate the risk. A residual risk may be known but is not completely controllable (i.e., not fully mitigated), or, it may be unknown. A residual risk is assumed by the Business Owner as the risk for providing the capability/service.
Supplemental Guidance	*Supplemental Guidance* provides non-prescriptive, additional information for a specific security control. Organizations can apply the supplemental guidance as appropriate, when defining, developing, and/or implementing security controls. The supplemental guidance can provide important considerations for implementing security controls in the context of operational environments, mission/business requirements, or assessments of risk and can also explain the purpose or meaning of controls.

Appendix E. Omitted and Not-Selected Controls and Control Enhancements

An omitted control is a control, with associated control enhancements, from NIST SP 800-53r4, that has been deemed discretionary for implementation within CMS or withdrawn by NIST. The discretionary controls are typically associated with environments with far more stringent protection needs such as national security.

Control enhancements that are under controls identified in the table below as *Omitted* also qualify as *Omitted*. If a Business owner wishes to select and implement a control enhancement under an omitted control, per NIST SP 800-53r4, the control itself must be addressed.

Control Family	Omitted Controls
AC	AC-13 – Withdrawn AC-15 – Withdrawn AC-23 – Data Mining Protection AC-24 – Access Control Decisions AC-25 – Reference
AT	AT-5 – Withdrawn
AU	AU-13 – Monitoring for Information Disclosure AU-14 – Session Audit AU-15 – Alternate Audit Capability
CA	CA-4 – Withdrawn
CM	None
CP	CP-5 – Withdrawn CP-11 – Alternate Communications Protocols CP-12 – Safe Mode CP-13 – Alternative Security Mechanisms
IA	IA-9 – Service Identification and Authentication IA-10 – Adaptive Identification and Authentication IA-11 – Re-authentication
IR	None
MA	None
MP	None
PE	PE-7 – Withdrawn PE-19 – Information Leakage PE-20 – Asset Monitoring and Tracking
PL	PL-3 – Withdrawn PL-5 – Withdrawn PL-6 – Withdrawn PL-7 – Security Concept of Operations PL-9 – Central Management
PS	None
RA	RA-4 – Withdrawn

Control Family	Omitted Controls
	RA-6 – Technical Surveillance Countermeasures Survey
SA	SA-6 – Withdrawn SA-7 – Withdrawn SA-14 – Criticality Analysis SA-18 – Tamper Resistance and Detection SA-19 – Component Authenticity
SC	SC-9 – Withdrawn SC-11 – Trusted Path SC-14 – Withdrawn SC-16 – Transmission of Security Attributes SC-25 – Thin Nodes SC-26 – Honeypots SC-27 – Platform-Independent Applications SC-29 – Heterogeneity SC-30 – Concealment and Misdirection SC-31 – Covert Channel Analysis SC-33 – Withdrawn SC-34 – Non-Modifiable Executable Programs SC-35 – Honeyclients SC-36 – Distributed Processing and Storage SC-37 – Out-of-Band Channels SC-38 – Operations Security SC-40 – Wireless Link Protection SC-41 – Port and I/O Device Access SC-42 – Sensor Capability and Data SC-43 – Usage
SI	SI-9 – Withdrawn SI-13 – Predictable Failure Prevention SI-14 – Non-Persistence SI-15 – Information Output Filtering SI-17 – Fail-Safe
PM	None
AP	None
AR	None
DI	None
DM	None
IP	None
SE	None
TR	None
UL	None

Controls and control enhancements from NIST SP 800-53r4 that are associated with *Mandatory* and *Non-Mandatory* controls but are not included within this ARS are identified as *Not Selected*

by CMS. While such control enhancements have not been included within the ARS, they do offer additional protections that the Business Owner should consider. While a Business Owner can make a risk-based decision to implement these control enhancements, compliance with the control enhancements will not be tracked by CMS. Control enhancements that are selected by the Business Owner must be documented.

The table below provides an example of control enhancements for the first six controls under the access control family (i.e., AC-1 (Access Control Policy and Procedures), AC-2 (Account Management), AC-3 (Access Enforcement), AC-4 (Information Flow Enforcement), AC-5 (Separation of Duties) and AC-6 (Least Privilege):

- AC-1, AC-3, AC-5, and AC-7 have no *Mandatory* or *Non-Mandatory* control enhancements. Neither AC-1 nor AC-5 has control enhancements defined under NIST SP 800-53. However, AC-3 and AC-7 have one or more control enhancements defined. Since the control enhancement under AC-3 or AC-7 have not been selected as either *Mandatory* (under one or more FIPS 199 security categories) or *Non-Mandatory*, the control enhancements are *Not Selected* and included in the example.
- AC-2, AC-4, and AC-6 have control enhancements, one or more of which are required under one or more of the FIPS 199 security categories. Any control enhancement under AC-2, AC-4, or AC-6 that has not been defined as *Mandatory* or selected as *Non-Mandatory* is *Not Selected* and included in the below example.
- Control enhancements under controls identified in the table above as Omitted also qualify as Omitted. They are also not selected. If a Business owner wishes to select a control enhancement under an omitted control, the control itself must be addressed.

See NIST SP 800-53r4 and the HHS IS2P for complete lists of controls and control enhancements.

Control Family	Controls	Control Enhancement Title
AC	AC-1	No control enhancements
	AC-2(6)	Account Management | Dynamic Privilege Management
	AC-2(7)	Account Management | Role-Based Schemes
	AC-2(8)	Account Management | Dynamic Account Creation
	AC-3(1)	Access Enforcement | Restricted Access to Privileged Functions
	AC-3(2)	Access Enforcement | Dual Authorization
	AC-3(3)	Access Enforcement | Mandatory Access Control
	AC-3(4)	Access Enforcement | Discretionary Access Control
	AC-3(5)	Access Enforcement | Security-Relevant Information
	AC-3(7)	Access Enforcement | Role-Based Access Control
	AC-3(8)	Access Enforcement | Revocation of Access Authorizations
	AC-3(10)	Access Enforcement | Audited Override of Access Control Mechanisms
	AC-4(1)	Information Flow Enforcement | Object Security Attributes
	AC-4(2)	Information Flow Enforcement | Processing Domains
	AC-4(3)	Information Flow Enforcement | Dynamic Information Flow Control

Control Family	Controls	Control Enhancement Title
	AC-4(4)	Information Flow Enforcement | Content Check Encrypted Information
	AC-4(5)	Information Flow Enforcement | Embedded Data Types
	AC-4(6)	Information Flow Enforcement | Metadata
	AC-4(7)	Information Flow Enforcement | One-Way Flow Mechanisms
	AC-4(9)	Information Flow Enforcement | Human Reviews
	AC-4(10)	Information Flow Enforcement | Enable / Disable Security Policy Filters
	AC-4(11)	Information Flow Enforcement | Configuration of Security Policy Filters
	AC-4(13)	Information Flow Enforcement | Decomposition into Policy-Relevant Subcomponents
	AC-4(14)	Information Flow Enforcement | Security Policy Filter Constraints
	AC-4(19)	Information Flow Enforcement | Validation of Metadata
	AC-4(20)	Information Flow Enforcement | Approved Solutions
	AC-4(22)	Information Flow Enforcement | Access Only
	AC-5	No control enhancements
	AC-6(4)	Least Privilege | Separate Processing Domains
	AC-6(6)	Least Privilege | Privileged Access by Non-Organizational Users
	AC-6(8)	Least Privilege | Privilege Levels for Code Execution
	AC-7(2)	Unsuccessful Logon Attempts | Purge / Wipe Mobile Device

Appendix F. Control and Control Enhancement Implementation Customization/Tailoring

This section provides examples of customizing implementation of controls and control enhancements.

F.1 CMS Tailoring Example: Customizing a Control or Control Enhancement Implementation

Table 4 is an extraction from Control AC-2 (Account Management) and associated FIPS 199 Implementation Standards, and provides an example on how tailoring may be leveraged to better meet mission/system needs.[19] This example is for a fictitious program known as CMS XYZ that provides an interface for beneficiaries and providers.

Table 4: Example ARS Control/Control Enhancement Implementation Customization

Control from ARS	The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary; . . . c. Establishes conditions for group and role membership; . . . e. Requires approvals by defined personnel or roles (defined in the applicable security plan) for requests to create information system accounts; . . . j. Reviews accounts for compliance with account management requirements at least every 90 days for High and Moderate systems or 365 days for Low systems; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. Implementation Standards (High, Moderate, & Low): . . . STD.3 Regulate the access provided to contractors and define security requirements for contractors. . . . STD.6 Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.
Tailored control implementation (e.g., private implementation details)	The CMS XYZ Program: a. Requires the following types of information system accounts to support CMS XYZ Program missions/business functions: • Individual/Organizational user accounts (federal and contractor employees), • System accounts (required by underlying operating system), • Application accounts (required by installed applications), • Guest/anonymous accounts (general users such as beneficiaries and providers) • Emergency and Temporary accounts (to provide emergency/temporary access) Shared/group accounts are not permitted under the XYZ Program

[19] Key phrases within the control and implementation standard are underlined. These indicate actions that the System/Business owner will need to take (e.g., definition of system-specific limits/requirements, identification of personnel) within the program's SSP.

	. . . c. The following group and role memberships apply to the CMS XYZ Program; • Group/roles associated with individual/organizational users: a. Employee I (maintaining/managing system) b. Employee II (elevated privileges for maintaining/managing system) c. Organizational Administration d. Application Administration • System group/roles (required by underlying Operating System) • Application group/roles (required by installed applications) • Guest/Anonymous (required for general user accounts for beneficiaries and providers) . . . e. Except for the general user account, the CMS XYZ Program Information System Security Officer (ISSO) or designee must approve all requests and modifications for an information system account before an account is created or group and role memberships are modified. • Emergency accounts may be authorized by the ISSO via phone. Approval must be logged within the Program XYZ system log book. • All approvals are logged. • The general user account is created by the general user (i.e., beneficiaries and providers) and is subject to the guidance defined under NIST SP 800-63 (latest) and Program XYZ processes and procedures for creating a general user account; . . . j. Reviews non-general user accounts for compliance with account management requirements no less often than every 30 days; and • General user accounts are reviewed every 90 days in accordance with NIST SP 800-63 (latest) and Program XYZ processes and procedures; k. Not applicable: Processes associated with shared/group account credentials are not applicable since shared/group accounts are not permitted. Program XYZ Customizations of Implementation Standards: STD.3 All Program XYZ contractors and subcontractors are subject to CMS acquisition and contractor personnel requirements. . . . STD.6 All Program XYZ systems will notify account managers within 24 hours when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.

The clauses listed in the bottom row have been customized to better describe how account management is implemented within the example program. In some cases, the implementation customizations defer to external processes and procedures. In another case, the customization is requiring a more frequent review cycle than CMS specified within the ARS. The customized implementation of the control and implementation standards would be included within the CMS XYZ Program SSP. Both the risk and deployed compensations associated with guest/anonymous accounts (e.g., for beneficiaries and providers) would be discussed within the XYZ Program ISRA.

F.2 CMS Tailoring Example: Identifying Controls and Control Enhancements as Not Applicable to a System Environment

Table 5 provides three examples of controls being identified as not applicable in the example environment. The first two are security controls (i.e., Control AC-18 (Wireless Access) and PE-13 (Emergency Lighting)). The last example, AR-7 (Privacy-Enhanced System Design and Development), is a privacy controls. This same process applies to control enhancements. As was

stated in the previous section, the examples are for a fictitious program known as CMS XYZ that provides an interface for beneficiaries and providers.

Table 5: Example Identifying Controls and Control Enhancements as *Not Applicable* to a System Environment

Security control from ARS	The organization monitors for unauthorized wireless access to information systems and prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If wireless access is authorized, the organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; b. Authorizes wireless access to the information system prior to allowing such connections; c. The organization ensures that: 1. The CMS CIO must approve and distribute the overall wireless plan for his or her respective organization; 2. Organizations adhere to the HHS Standard for IEEE 802.11 Wireless Local Area Network (WLAN); and 3. Mobile and wireless devices, systems, and networks are not connected to wired HHS/CMS networks except through appropriate controls (e.g., VPN port) or unless specific authorization from HHS/CMS network management has been received.
Control implementation (e.g., allocation status & private implementation details)	Not Applicable: The CMS XYZ Program does not permit the use of wireless technology within its facilities.

Security control from ARS	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.
Control implementation (e.g., allocation status & private implementation details)	Inherited: The CMS XYZ Program is entirely housed within Baltimore Data Center (BDC) facilities. All lighting is managed and maintained by BDC. It should be noted that BDC performs regular (quarterly) tests to ensure emergency lighting is operational.

Privacy control from ARS	The organization designs information systems to support privacy by automating privacy controls to the extent feasible, integrating and meeting privacy requirements throughout the CMS Life Cycle, and incorporating privacy concerns into reviews of significant changes to HHS/CMS systems, networks, physical environments, and other agency infrastructures. The organization also conducts periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act, the organization's privacy policy, and any other legal or regulatory requirements
Control implementation (e.g., allocation status & private implementation details)	Not Applicable: The CMS XYZ Program does not process, store, or transmit PII nor PHI.

This page intentionally blank.