| CMS Manual System | **Department of Health & Human Services (DHHS)** |
|---|---|
| Pub 100-25 Information Security Acceptable Risk Safeguards | **Centers for Medicare & Medicaid Services (CMS)** |
| **Transmittal 1** | **Date: May 24, 2011** |
| | **Change Request 7104** |

**SUBJECT: Information Security Acceptable Risk Safeguards**

**I. SUMMARY OF CHANGES:** CMS has determined that the CMS Information Security Acceptable Risk Safeguards must be incorporated into the CMS manual process.

**EFFECTIVE DATE: August 31, 2010**
**IMPLEMENTATION DATE: June 24, 2011**

*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 |
|---|---|
| N | 10.0/Introduction |
| N | 20.0/Purpose |
| N | 30.0/Scope |
| N | 40.0/How to Use the Appendices |
| N | 40.0/4.1/CMSR Appendices |
| N | 40.0/4.2/E-Authentication Appendix |
| N | 50.0/CMSR Structure |
| N | 50.1/CMSR Family Numbering and Description |
| N | 50.2/Control Requirements |
| N | 50.2.1/Baseline Control |
| N | 50.2.2/Enhancement Control |
| N | 50.2.3/Implementation Standard |
| N | 50.2.4/Guidance |
| N | 50.2.5/Applicability |
| N | 50.2.6/References |
| N | 50.2.7/Related Control Requirements |
| N | 50.3/Assessment Procedures |
| N | 50.3.1/Assessment Objective |
| N | 50.3.2/Assessment Methods and Objects |
| N | 60.0/References |
| N | Appendix A/CMSR High Impact Level Data |
| N | Appendix A/1.0/Access Control (AC) - Technical |
| N | Appendix A/2.0/Awareness and Training (AT) - Operational |
| N | Appendix A/3.0/Audit and Accountability (AU) - Technical |
| N | Appendix A/4.0/Security Assessment and Authorization (CA) - Management |
| N | Appendix A/5.0/Configuration Management (CM) - Operational |
| N | Appendix A/6.0/Contingency Planning (CP) - Operational |
| N | Appendix A/7.0/Identification and Authentication (IA) - Technical |
| N | Appendix A/8.0/Incident Response (IR) - Operational |
| N | Appendix A/7.0/Identification and Authentication (IA) - Technical |
| N | Appendix A/9.0/Maintenance (MA) - Operational |
| N | Appendix A/10.0/Media Protection (MP) - Operational |

| | |
|---|---|
| N | Appendix A/11.0/Physical and Environmental Protection (PE) - Operational |
| N | Appendix A/12.0/Planning (PL) - Management |
| N | Appendix A/13.0/Personnel Security (PS) - Operational |
| N | Appendix A/14.0/Risk Assessment (RA) - Management |
| N | Appendix A/15.0/System and Services Acquisition (SA) - Management |
| N | Appendix A/16.0/System and Communications Protection (SC) - Technical |
| N | Appendix A/17.0/System and Information Integrity (SI) - Operational |
| N | Appendix B/CMSR Moderate Impact Level Data |
| N | Appendix B/1.0/Access Control (AC) - Technical |
| N | Appendix B/2.0/Awareness and Training (AT) - Operational |
| N | Appendix B/3.0/Audit and Accountability (AU) - Technical |
| N | Appendix B/4.0/Security Assessment and Authorization (CA) - Management |
| N | Appendix B/5.0/Configuration Management (CM) - Operational |
| N | Appendix B/6.0/Contingency Planning (CP) - Operational |
| N | Appendix B/7.0/Identification and Authentication (IA) - Technical |
| N | Appendix B/8.0/Incident Response (IR) - Operational |
| N | Appendix B/9.0/Maintenance (MA) - Operational |
| N | Appendix B/10.0/Media Protection (MP) - Operational |
| N | Appendix B/11.0/Physical and Environmental Protection (PE) - Operational |
| N | Appendix B/12.0/Planning (PL) - Management |
| N | Appendix B/13.0/Personnel Security (PS) - Operational |
| N | Appendix B/14.0/Risk Assessment (RA) - Management |
| N | Appendix B/15.0/System and Services Acquisition (SA) - Management |
| N | Appendix B/16.0/System and Communications Protection (SC) - Technical |
| N | Appendix B/17.0/System and Information Integrity (SI) - Operational |
| N | Appendix C/CMSR Low Impact Level Data |
| N | Appendix C/1.0/Access Control (AC) - Technical |
| N | Appendix C/2.0/Awareness and Training (AT) - Operational |
| N | Appendix C/3.0/Audit and Accountability (AU) - Technical |
| N | Appendix C/4.0/Security Assessment and Authorization (CA) - Management |
| N | Appendix C/5.0/Configuration Management (CM) - Operational |
| N | Appendix C/6.0/Contingency Planning (CP) - Operational |
| N | Appendix C/7.0/Identification and Authentication (IA) - Technical |

| | |
|---|---|
| N | Appendix C/8.0/Incident Response (IR) - Operational |
| N | Appendix C/9.0/Maintenance (MA) - Operational |
| N | Appendix C/10.0/Media Protection (MP) - Operational |
| N | Appendix C/11.0/Physical and Environmental Protection (PE) - Operational |
| N | Appendix C/12.0/Planning (PL) - Management |
| N | Appendix C/13.0/Personnel Security (PS) - Operational |
| N | Appendix C/14.0/Risk Assessment (RA) - Management |
| N | Appendix C/15.0/System and Services Acquisition (SA) - Management |
| N | Appendix C/16.0/System and Communications Protection (SC) - Technical |
| N | Appendix C/17.0/System and Information Integrity (SI) - Operational |
| N | Appendix D/CMSR e-Authentication |
| N | Appendix D/1.0/Introduction |
| N | Appendix D/2.0/Purpose |
| N | Appendix D/3.0/E-Authentication Model |
| N | Appendix D/4.0/Technical Requirements by Assurance Level |
| N | Appendix D/4.1/Registration and Identity Proofing |
| N | Appendix D/4.2/Authentication and Mechanism Requirements |
| N | Appendix D/4.2.1/Token |
| N | Appendix D/4.3/Summary of Technical Requirements |

**III. FUNDING:**
**For Fiscal Intermediaries (FIs), Regional Home Health Intermediaries (RHHIs) and/or Carriers:**
Funding for implementation activities will be provided to contractors through the regular budget process.

**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**

**Unless otherwise specified, the effective date is the date of service.*

# Attachment - Business Requirements

| Pub. 100-25 | Transmittal: 1 | Date: May 24, 2011 | Change Request: 7104 |
|---|---|---|---|

**SUBJECT: Information Security Acceptable Risk Safeguards**

**Effective Date**: August 31, 2010

**Implementation Date:** June 24, 2011

## I. GENERAL INFORMATION

**A. Background:** CMS has determined that the CMS Information Security Acceptable Risk Safeguards (ARS) must be incorporated into the CMS manual process. In addition, the ARS is being updated to include updates from the NIST SP 800-53 Revision 3, dated August 2009.

**B. Policy:** The Federal Information Security Management Act of 2002 requires the development of minimum security requirements for information and information systems. In response the National Institutes of Standards and Technology (NIST) published Federal Information Processing Standard (FIPS) 200, which all Federal agencies must comply with. FIPS 200 designates the use of NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations, as amended, in meeting its requirements. The ARS is the CMS implementation of NIST SP 800-53.

## II. BUSINESS REQUIREMENTS TABLE

*Use"Shall" to denote a mandatory requirement*

| Number | Requirement | Responsibility (place an "X" in each applicable column) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A/B MAC | DME MAC | FI | CARRIER | RHHI | Shared-System Maintainers | | | | OTHER |
| | | | | | | | FISS | MCS | VMS | CWF | |
| 7104.1 | All CMS information, information systems, IT activities, and IT assets owned, leased, controlled, or used by CMS, CMS' agents, contractors, or other business partners on behalf of CMS shall comply with the controls defined in the CMS Information Security Acceptable Risk Safeguards as the minimum security requirements for all CMS information and information systems. | X | X | X | X | X | | | | | All CMS information, information systems, IT activities, and IT |

| Number | Requirement | Responsibility (place an "X" in each applicable column) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A/B MAC | DME MAC | FI | CARRIER | RHHI | Shared-System Maintainers | | | | OTHER |
| | | | | | | | FISS | MCS | VMS | CWF | |
| | | | | | | | | | | | assets owned, leased, controlled, or used by CMS, CMS' agents, contractors, or other business partners on behalf of CMS. |

## III. PROVIDER EDUCATION TABLE

| Number | Requirement | Responsibility (place an "X" in each applicable column) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A/B MAC | DME MAC | FI | CARRIER | RHHI | Shared-System Maintainers | | | | OTHER |
| | | | | | | | FISS | MCS | VMS | CWF | |
| | **None.** | | | | | | | | | | |

## IV. SUPPORTING INFORMATION

**Section A: For any recommendations and supporting information associated with listed requirements, use the box below: N/A**
*Use "Should" to denote a recommendation.*

| X-Ref Requirement Number | Recommendations or other supporting information: |
|---|---|
| | |

**Section B: For all other recommendations and supporting information, use this space: N/A**

## V. CONTACTS

**Pre-Implementation Contact(s):** Jason King, (410) 786-7578

**Post-Implementation Contact(s):** ciso@cms.hhs.gov
Contact your Contracting Officer's Technical Representative (COTR) or Contractor Manager, as applicable.

## VI. FUNDING

**Section A: For *Fiscal Intermediaries (FIs), Regional Home Health Intermediaries (RHHIs),* and/or *Carriers*:**

Funding for implementation activities will be provided to contractors through the regular budget process.

**Section B: *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.

# Information Security (IS)
# Acceptable Risk Safeguards (ARS)

***(Rev.1, 05-24-11)***

## Table of Contents


10.0 Introduction
20.0 Purpose
30.0 Scope
40.0 How to Use the Appendices
  40.1 CMSR Appendices
  40.2 E-Authentication Appendix
50.0 CMSR Structure
  50.1 CMSR Family Numbering and Description
  50.2 Control Requirements
    50.2.1 Baseline Control
    50.2.2 Enhancement Control
    50.2.3 Implementation Standard
    50.2.4 Guidance
    50.2.5 Applicability
    50.2.6 References
    50.2.7 Related Control Requirements
  50.3 Assessment Procedures
    50.3.1 Assessment Objective
    50.3.2 Assessment Methods and Objects
60.0 References


## List of Tables


Table 50-1. CMSR Security Control Family Descriptions
Table 50-2. Implementation Standards for CMSR AC-20
Table 50-3. Handling of Special Information


## Appendices


Appendix A CMS Minimum Security Requirements for High Impact Level Data
Appendix B CMS Minimum Security Requirements for Moderate Impact Level Data
Appendix C CMS Minimum Security Requirements for Low Impact Level Data
Appendix D e-Authentication Standard

# 10.0 Introduction

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The Centers for Medicare & Medicaid Services (CMS) Information Security (IS) Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR) contain a broad set of required security standards based upon the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, dated August 2009, and NIST 800-63 Version 1.0.2, Electronic Authentication Guideline, dated, April 2006 as well as additional standards based on CMS policies, procedures, and guidance, other federal and non-federal guidance resources and industry leading security practices. This document provides guidance to CMS and its contractors as to the minimum level of required security controls that must be implemented to protect CMS' information and information systems.

Incorporating controls cataloged in this document will ensure that all CMS systems meet a minimum level of IS. However, many CMS systems, particularly those that are mission-critical or that are available to Internet users, will require additional security protections as part of CMS' implementation requirements such as the CMS Internet Architecture. This document describes architecture standards that must be in place for Internet-facing systems. Business Owners should refer to http://www.cms.hhs.gov/SystemLifecycleFramework/ to ensure that all CMS information system development requirements are met.

A system may be required to meet additional, higher-level or more rigorous, information protection requirements as mandated by specific federal, legal, program, or accounting sources. For example, the CMSR control "Audit and Accountability" (AU) AU-11 Audit Retention, states that for all systems "the audit records will be retained for ninety (90) days and then archived for one (1) year." However, the National Archives and Records Administration (NARA) has determined that Audit Files (NC1-440-78-1, Item B) be retained for four (4) years after completion of an audit. Therefore, if these logs were utilized as part of an audit, the NARA requirements would take precedence. The CMS system must be developed to meet these higher-level standards where applicable. The ARS shall not be construed to relieve or waive these other standards.

It is important to note that the ARS does not address specific business process requirements that ensure business requirements are fulfilled. The goal of the CMSRs is to provide a baseline of minimally required internal/external IS controls. It is the responsibility of the Business Owner of CMS systems, with direction provided by the Office of Information Services (OIS), to ensure that all applicable internal/external IS controls are incorporated into CMS systems. Business Owners must document and certify the incorporated controls in their respective CMS System Security Plan (SSP) and identify any risks in the corresponding CMS Information Security Risk Assessment (IS RA) for their system.

## 20.0 Purpose

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

Protecting and ensuring the confidentiality, integrity, and availability (CIA) for all of CMS' information and information systems is the primary purpose of the IS program. The ARS complies with the CMS Policy for the Information Security Program (PISP) by providing a defense-in-depth security structure along with a least-privilege, need-to-know basis for all information access.

The CMSRs within the ARS are not intended to be an all-inclusive list of security controls nor are they intended to replace a Business Owner's due diligence to incorporate additional controls to mitigate risk. The CMSRs are the minimum security requirements to be considered and employed where applicable throughout the risk management process and the CMS Integrated Information Technology (IT) Investment & Life Cycle Framework (a.k.a. "Framework").

## 30.0 Scope

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

All CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions and performing work on behalf of CMS shall observe the baseline policy statements described in the PISP and the complementary controls defined in the ARS as the minimum security requirements for all CMS information and information systems.

The Business Owner, assisted by the System Developer/Maintainer, has primary responsibility for evaluating the ARS and determining the appropriateness of the CMSRs for their system and ensuring their proper implementation. Unless a CMSR is stated as "Optional" or is specifically omitted from the specified CMSR, the CMSR is required.

A Business Owner may choose to strengthen the control beyond its system security level requirement to provide the best possible protection of CMS' information and information systems. In some cases, a Business Owner may not need to directly implement some specific controls as long as they can adequately demonstrate (and document) that the requirement is satisfied by a parent system.

Sometimes security controls cannot be implemented even at the minimum level due to resource issues such as funding restrictions, personnel constraints or hardware/software limitations. Alternative or compensating controls can be implemented to reduce the risk to CMS: its information, information systems, assets and reputation. This must be considered as part of risk management process though the CMS IS C&A Program. The alternative or compensating controls must be documented in the SSP, any remaining risk must be defined in the IS RA and

both must be approved by the Chief Information Officer (CIO) or his/her designated representative.

## 40.0 How to Use the Appendices

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The CMSRs provided in Appendices A, B, and C, along with the e-Authentication controls in Appendix D, are a detailed resource for understanding all aspects of the CMS defined security controls.

## 40.1 CMSR Appendices

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

Each CMSR Appendix is a set of security controls based on a CMS System Security Level (i.e., High, Moderate, and Low) as established by Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. Each Business Owner is required to determine their system's security level according to CMS System Security and e-Authentication Assurance Levels by Information Type, (http://www.cms.hhs.gov/InformationSecurity/Downloads/ssl.pdf) and use that designation to select the appropriate CMSR appendix for defining their minimum set of required security controls. The CMSRs Appendices are:

- Appendix A: CMS Minimum Security Requirements for High Impact Level Data
- Appendix B: CMS Minimum Security Requirements for Moderate Impact Level Data
- Appendix C: CMS Minimum Security Requirements for Low Impact Level Data

Each Appendix includes baseline and enhancement controls, and associated amplifying information, for the indicated security level. The CMSRs include:

- Control text (Baseline and Enhancement Controls)
- Additional CMS or data-type specific standards (e.g., CMS defined variables) to which the control must meet (Implementation Standards)
- Additional guidance for clarifying the control (Guidance)
- CMS defined exceptions to specific controls (Applicability)
- The specific laws, standards, or mandates from which the control originated (Reference)
- Related controls (Related Control Requirements)

- Recommended objects and methodologies for assessing compliance with each control. (Assessment Procedure)

While each CMSR contains a significant amount of associated information, it should be noted that this information is provided to the user in order to maximize understanding of, not only the controls, but also the expectations for reaching compliance and the methodologies that will be used to verify compliance.

## 40.2 E-Authentication Appendix

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

CMSR IA-2 is the baseline control for e-Authentication. Included with the baseline are the enhancements establishing the minimum control requirements. The specific implementation of local and remote e-Authentication controls are described in Appendix D, e-Authentication Standard, as determined by the CMS System Security and e-Authentication Assurance Levels by Information Type, (http://www.cms.hhs.gov/InformationSecurity/Downloads/ssl.pdf).

## 50.0 CMSR Structure

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

## 50.1 CMSR Family Numbering and Description

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The security controls have a well-defined organization and structure. They are organized into 18 control families within 3 classes (management, operational, and technical) for ease of use in the security control selection and specification process. The families are established by NIST SP 800-53, *and are* in alignment with the 18 security-related areas specified in FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each of the 18 security control families. It should be noted that some of the controls within a family may have characteristics that can be in more than one class. The class that is predominately supported by the family is the class designation for the entire family. The Program Management (PM) family is summarized in the PISP and is not included in the current CMSRs. Table 5-1 summarizes the 17 security control families and the two-character identifier used in the CMSRs:

**Table 50-1. CMSR Security Control Family Descriptions**

| Family (and Identifier) | Class | Description |
|---|---|---|
| Access Control (AC) | Technical | The standards listed in this section focus on how the organization shall limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. |
| Awareness and Training (AT) | Operational | The standards listed in this section focus on how the organization shall: (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. |
| Audit and Accountability (AU) | Technical | The standards listed in this section focus on how the organization shall: (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) | Management | The standards listed in this section focus on how the organization shall: (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) | Operational | The standards listed in this section focus on how the organization shall: (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) | Operational | The standards listed in this section focus on how the organization shall establish, maintain, and effectively 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. |

| Family (and Identifier) | Class | Description |
|---|---|---|
| Identification and Authentication (IA) | Technical | The standards listed in this section focus on how the organization shall identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| Incident Response (IR) | Operational | The standards listed in this section focus on how the organization shall: (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) | Operational | The standards listed in this section focus on how the organization shall: (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) | Operational | The standards listed in this section focus on how the organization shall: (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. |
| Physical and Environmental Protection (PE) | Operational | The standards listed in this section focus on how the organization shall: (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) | Management | The standards listed in this section focus on how the organization shall 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) | Operational | The standards listed in this section focus on how the organization shall: (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. |

| Family (and Identifier) | Class | Description |
|---|---|---|
| Risk Assessment (RA) | Management | The standards listed in this section focus on how the organization shall 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) | Management | The standards listed in this section focus on how the organization shall: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate IS 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) | Technical | The standards listed in this section focus on how the organization shall: (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 IS within organizational information systems. |
| System and Information Integrity (SI) | Operational | The standards listed in this section focus on how the organization shall: (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. |

## 50.2 Control Requirements

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The CMS security control structure consists of the Baseline or Enhancement section, Guidance section, Applicability section, References section, Related Requirements section and Assessment Procedures section. In addition, the baseline will have a sub-section for Implementation Standards which will only be associated with that baseline.

The CMS-tailored baseline security controls (i.e., CMS PISP policy statements) serve as the starting point for organizations in determining the appropriate controls and countermeasures necessary to protect their information systems.

### 50.2.1 Baseline Control

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The Baseline control is the concise statement specifying the capability needed to protect a particular aspect of the CMS information or information system at that determined system security level.

Baseline controls are identified by security control Family ID and convey CMS PISP policy statements, which are based on NIST 800-53 and are:

- Identical across all three system levels
- Employ NIST numbering where direct correlations are made (e.g., AC-1, AC-2, AC-3…)
- Use CMS designators where a direct NIST correlation was not made (e.g., AC-CMS-1.)
- Ordered such that the CMS designators always follow the complete set of NIST designators and always restart the numbering of the CMS designator at 1 (e.g. AC-1, AC-2, AC-3, AC-4, AC-5, …AC-CMS-1)

The baseline section includes the following:

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

## 50.2.2 Enhancement Control

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

Enhancement controls supplement baseline controls to achieve the overall required level of protection in accordance with the system security level. Enhancements may only be required for higher system security level baselines but may be used to strengthen the level of protection provided in lower system security level systems, if deemed appropriate by the Business Owner.

The enhancement controls are structured the same as the baseline controls with the exception of implementation standards. Each enhancement section is as follows:

- Control Requirement
- Guidance (may not exist for all Enhancements)
- Applicability
- References
- Related Control Requirements
- Assessment Procedure
    - Assessment Objectives
    - Assessment Methods and Objects

## 50.2.3 Implementation Standard

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

When an implementation standard is indicated, it is only associated with a baseline control. The purpose of the implementation standard is to provide CMS tailored controls for implementation of the associated baseline.

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. Other implementation standards are based on specific types of data such as Protected Health Information (PHI), Personally Identifiable Information (PII) or Federal Tax Information (FTI).

For example, AC-20’s second implementation standard, at the High system security level states:

"(For PII only) Only organization owned computers and software can be used to process, access, transmit, and store PII."

This particular implementation standard is used by organizations responsible for PII information.

Similar implementation standards exist and apply for organizations responsible for PHI or FTI data. All other implementation standards, where no "(For XXX only)" is indicated, are CMS implementation controls that shall be implemented at the designated system security level for all CMS information and information systems.

Table 50-2 shows an example of the implementation standard associated with CMSR AC-20. Implementation standard item 1 is a CMS-specified control which applies to all CMS information and information systems. Item 2 is specifically designated for those organizations responsible for PII and must be followed for implementation, assessment and audit.

Note: When referenced outside of the context of the specific CMSR, these implementation standards may be referred to (more specifically) as AC-20.Std.1 and AC-20.Std.2.

**Table 50-2. Implementation Standards for CMSR AC-20**

| Implementation Standard(s) |
|---|
| 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.<br>2. For PII only) Only organization owned computers and software can be used to process, access, and store PII. |

Table 50-3 provides definitions for PII, PHI and FTI. Organizations responsible for these types of information must provide additional safeguards as defined in the implementation standards.

**Table 50-3. Handling of Special Information**

| Term | Definition |
|---|---|
| Personally Identifiable Information (PII) | Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual. |
| Protected Health Information (PHI) or Individually Identifiable Health Information | Individually identifiable health information that is:<br>(i) transmitted by electronic media,<br>(ii) maintained in electronic media, or<br>(iii) transmitted or maintained in any other form or medium. (HIPAA)<br>NOTE: PHI excludes individually identifiable health information in employment records held by a covered HIPAA entity in its role as employer. |
| Federal Tax Information (FTI) | Generally, Federal Tax Returns and return information are confidential, as required by IRC Section 6103. The information is used by the IRS to ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality. |

### 50.2.4 Guidance

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The CMSR may include additional Guidance to explain the intent of the control. In some cases these include specific CMS desires or recommendations, or may refer to other CMS or NIST publications for further guidance. It is a good security practice to refer to the guidance and procedures for additional information to facilitate the organization meeting the CMS security requirements.

### 50.2.5 Applicability

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

All CMSRs must be met unless a control requirement is specified as an exception or optional in the Applicability section. If a particular contract/entity type is not listed below, all CMSRs apply until such time as an evaluation is made by the CMS Chief Information Security Officer (CISO), and the CMSRs are updated to reflect the updated applicability exception list. The current contract/entity types are:

- ABMAC – A/B Medicare Administrative Contractor
- COB – Coordination of Benefits
- CWF – Common Working File [Host]
- DC – Data Center
- DMEMAC – Durable Medical Equipment Medicare Administrative Contractor
- EDC – Enterprise Data Center
- PartA – Part A Fiscal Intermediary
- PartB – Part B Carrier
- PSC – Program Safeguard Contractor
- QIC – Quality Integrity Contractor
- RAC – Recovery Audit Contractor
- SS – Standard System [Maintainer]

- ZPIC – Zone Program Integrity Contractor

### 50.2.6 References

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The references section identifies the source documents and section or paragraph designations that are the basis or source for the applicable CMSR. For example an IRS reference would look like: IRS-1075: 5.6.3.2#1. From this example:

- The IRS-1075 is the publication.
- The 5.6.3.2#1 portion is the section with sub-paragraphs leading to the applicable reference used for the control requirement.

### 50.2.7 Related Control Requirements

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

Many, but not all, CMSRs may be related to one or more other CMSR. When addressing some CMSRs, it may be important that their responses during an assessment or audit be consistent with one or more related CMSRs. At the very least, organizations shall take care to ensure that related CMSR responses do not conflict. While every effort was made to identify related CMSRs, other unidentified relationships may exist that are unique to a particular system, contract type, or organization.

## 50.3 Assessment Procedures

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The assessment procedures, including Assessment Objectives, and Assessment Methods and Objects, help determine if the security controls in the information system are effective in their application (i.e., implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system). They provide a foundation to support the security certification process. The "Assessment Procedure" consists of a set of procedural steps that are designated to achieve one or more objectives by applying methods to assessment objects.

### 50.3.1 Assessment Objective

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The "Assessment Objectives" include a set of determination statements ("Determine if…") related to the particular security control under assessment. The determination statements are

closely linked to the content of the security control (i.e., the security control functionality) to ensure traceability of assessment results back to the fundamental control requirements.

Assessment objectives establish the expectations for security control assessments based on the assurance requirements defined in the security 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 security control effectiveness. Each of the Assessment Objective determination statements is either traceable to requirements in the baseline or enhancement security control, or the guidance. This ensures that all aspects of the security control are assessed and that any weaknesses or deficiencies in the control can be identified and remediation actions taken.

It should be noted that the Test Scripts for Information Security (IS) Assessments, http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp, utilize the same Assessment Objective in its explanation of the expectations of security assessments by system security level. Organizations are expected use the Test Scripts for Information Security (IS) Assessments during their assessments.

### 50.3.2 Assessment Methods and Objects

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The assessment methods define the nature of the assessor's actions and include Examine, Interview, and Test. The assessment object identifies the specific item being assessed including specifications, mechanism, activities and individuals. The application of an assessment procedure to a security control produces assessment findings. These assessment findings are subsequently used in helping to determine the overall effectiveness of the control. A detailed explanation of the three (3) assessment methods can be found in the Test Scripts for Information Security (IS) Assessments.

## 60.0 References

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

The CMS IS program and ARS were developed in accordance with Federal mandates and CMS requirements for the handling and processing of CMS' information and information systems. The CMS IS web site at http://www.cms.hhs.gov/InformationSecurity/12_Laws_Regs.asp provides a list of applicable laws across the program. Some additional references are provided below:

- Public Law 74-271, Social Security Act, as amended
http://www.ssa.gov/OP_Home/ssact/ssact.htm.htm

- Public Law 93-579, The Privacy Act of 1974, as amended
http://www.usdoj.gov/foia/privstat.htm

- Public Law 104-13, Paperwork Reduction Act of 1995, as amended
http://www.fws.gov/policy/library/rgpl104-13.pdf

- 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://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ173.108.pdf

- Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability, 5CFR731
http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html

- United States Code Title 44 Chapter 33—Disposal of Records
http://www.archives.gov/about/laws/disposal-of-records.html

- GAO-09-232G, Federal Information System Controls Audit Manual (FISCAM), February 2, 2009
http://www.gao.gov/new.items/d09232g.pdf

- OMB Circulars can be found at the CMS web site or at:
http://www.whitehouse.gov/omb/circulars/index.html

- Homeland Security Presidential Directives can be found at:
http://www.dhs.gov/xabout/laws/editorial_0607.shtm

- Executive Orders can be found at:
http://www.archives.gov/federal-register/executive-orders/disposition.html

- A list of NIST special publications and FIPS publications can be found at:
http://csrc.nist.gov/publications/

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

Additional CMS documents were used as references in the development of this manual. The CMS IS web site at http://www.cms.hhs.gov/InformationSecurity/ provides a list of applicable CMS documents across the IS program.

# CMS Information Security (IS)
# Acceptable Risk Safeguards (ARS)

## Appendix A - CMSR High Impact Level Data

***(Rev.1, 05-24-11)***

## Table of Contents


1.0 Access Control (AC) – Technical 1

2.0 Awareness and Training (AT) – Operational 47

3.0 Audit and Accountability (AU) – *Technical* 55

4.0 Security Assessment and Authorization (CA) – *Management* 78

5.0 Configuration Management (CM) – *Operational* 95

6.0 Contingency Planning (CP) – *Operational* 126

7.0 Identification and Authentication (IA) – *Technical* 154

8.0 Incident Response (IR) – *Operational* 171

9.0 Maintenance (MA) – *Operational* 187

*10.0* Media Protection (MP) – *Operational* 201

11.0 Physical and Environmental Protection (PE) – *Operational* 219

12.0 Planning (PL) – *Management* 244

13.0 Personnel Security (PS) – *Operational* 252

14.0 Risk Assessment (RA) – *Management* 261

15.0 System and Services Acquisition (SA) – *Management* 272

16.0 System and Communications Protection (SC) – *Technical* 297

17.0 System and Information Integrity (SI) – *Operational* 334

# 1.0 ACCESS CONTROL (AC) – TECHNICAL

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **AC-1 – Access Control Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AS-1, SM-1, SM-3; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents access control policy; | | |

the organization access control policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities;

the organization develops and formally documents access control procedures;

the organization access control procedures facilitate implementation of the access control policy and associated access controls;

the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities;

the organization reviews/updates the access control policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Access control policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with access control responsibilities.

| AC-2 – Account Management (High) | | |
|---|---|---|
| **Control**<br>The organization manages information system accounts, including:<br>a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);<br>b. Establishing conditions for group membership;<br>c. Identifying authorized users of the information system and specifying access privileges;<br>d. Requiring appropriate approvals for requests to establish accounts;<br>e. Establishing, activating, modifying, disabling, and removing accounts;<br>f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;<br>g. Notifying account managers 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;<br>h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;<br>i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and<br>j. Reviewing accounts using the frequency specified in Implementation Standard 1.<br>**Implementation Standard(s)**<br>1. Review information system accounts within every ninety (90) days and require annual certification.<br>2. Remove or disable default user accounts. Rename active default accounts.<br>3. Implement centralized control of user access administrator functions.<br>4. Regulate the access provided to contractors and define security requirements for contractors. | | |
| **Guidance**<br>The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AC-4, AS-2, AS-4, BP-3, SD-2, SM-4; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AC-2.1**

**Assessment Objective**

Determine if:
the organization manages information system accounts, including;
- identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
- establishing conditions for group membership;
- identifying authorized users of the information system and specifying access privileges;
- requiring appropriate approvals for requests to establish accounts;
- establishing, activating, modifying, disabling, and removing accounts;
- specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- notifying account managers 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;
- deactivating: (a) temporary accounts that are no longer required; and (b) accounts of terminated or transferred users;
- granting access to the system based on: (a) a valid access authorization; (b) intended system usage; and (c) other attributes as required by the organization or associated missions/business functions;

the organization reviews information system accounts in accordance with the frequency specified in Implementation Standard 1.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing account management; security plan; list of active 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.

**Interview:** Organizational personnel with account management responsibilities.

**AC-2(1) – Enhancement (High)**

**Control**

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

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#2.1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-2(1).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms to support information system account management functions.

**Assessment Methods And Objects**

**Examine:** Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing account management functions.

**AC-2(2) – Enhancement (High)**

**Control**

The information system automatically terminates emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three hundred sixty-five (365) days.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#2.1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-2(2).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, a time period for each type of account after which the information system terminates temporary and emergency accounts;

the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.

**Assessment Methods And Objects**

**Examine:** Security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of active accounts; information system audit records; other relevant documents or records.

**Test:** Automated mechanisms implementing account management functions.

| AC-2(3) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The information system automatically disables inactive accounts after ninety (90) days. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#2.1 | **Related Controls**<br>**Requirement(s):** IA-4.Std.1 |
| **ASSESSMENT PROCEDURE: AC-2(3).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, a time period after which the information system disables inactive accounts;<br>the information system automatically disables inactive accounts after organization-defined time period.<br>**Assessment Methods And Objects**<br>**Examine:** Procedures addressing account management; 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; other relevant documents or records.<br>**Test:** Automated mechanisms implementing account management functions. | | |
| **AC-2(4) – Enhancement (High)** | | |
| **Control**<br>The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#2.1 | **Related Controls**<br>**Requirement(s):** |

| **ASSESSMENT PROCEDURE: AC-2(4).1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the information system automatically audits:<br>- account creation;<br>- modification;<br>- disabling;<br>- termination actions;<br>the information system notifies, as required, appropriate individuals.<br>**Assessment Methods And Objects**<br>**Examine:** Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.<br>**Test:** Automated mechanisms implementing account management functions. | | |
| **AC-2(7) – Enhancement (High)** | | |
| **Control**<br>The organization:<br>(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;<br>(b) Tracks and monitors privileged role assignments; and<br>(c) Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every seven (7) days to ensure that unauthorized accounts have not been created. | | |
| **Guidance**<br>Privileged roles include, for example, key management, network and system administration, database administration, web administration. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AC-2(7).1**

**Assessment Objective**

Determine if:
the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;

the organization tracks and monitors privileged role assignments;

the organization inspects administrator groups, root accounts and other system related accounts on demand, but at least once during the specified period to ensure that unauthorized accounts have not been created.

**Assessment Methods And Objects**

**Examine:** Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; information system audit records; audit tracking and monitoring reports; other relevant documents or records.

**Interview:** Organizational personnel with account management responsibilities.

**AC-3 – Access Enforcement (High)**

**Control**

The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

**Implementation Standard(s)**

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).
2. If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix D: E-authentication Standard.
3. Configure operating system controls to disable public "read" and "write" access to all system files, objects, and directories. Configure operating system controls to disable public "read" access to files, objects, and directories that contain sensitive information.
4. Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas.

**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) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

Encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative.

Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AS-1, AS-2, AS-3, AS-4, BP-2, BP-4, CM-3, DA-1, IN-2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3 | **Related Controls Requirement(s):** SC-13 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-3.1**

**Assessment Objective**

Determine if:

the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records.

**Test:** Automated mechanisms implementing access enforcement policy.

| AC-3(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>[Withdrawn: Incorporated into AC-6]. | | |
| **AC-4 – Information Flow Enforcement (High)** | | |
| **Control**<br>The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. | | |
| **Guidance**<br>Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) 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 content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-1, BP-2, BP-4, DA-1; IRS-1075: 5.6.3.2#2.2 | **Related Controls Requirement(s):** SC-7 |
| **ASSESSMENT PROCEDURE: AC-4.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines applicable policy for controlling the flow of information within the system and between interconnected systems;<br>the organization defines approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; | | |

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

**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.

**Test:** Automated mechanisms implementing information flow enforcement policy.

## AC-5 – Separation of Duties (High)

**Control**

The organization:
a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
b. Documents separation of duties; and
c. Implements separation of duties through assigned information system access authorizations.

**Implementation Standard(s)**

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

**Guidance**

Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, AS-3, AS-4, BP-4, SD-1, SD-2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-5.1**

**Assessment Objective**

Determine if:
the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;

the organization documents separation of duties;

the organization implements separation of duties through assigned information system access authorizations.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties.

**Test:** Automated mechanisms implementing separation of duties policy.

## AC-6 – Least Privilege (High)

**Control**

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

**Implementation Standard(s)**

1. Disable all file system access not explicitly required for system, application, and administrator functionality.
2. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.
3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value levels. Implement column-level access controls.
4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.
5. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If authorized, boot access is password protected.

**Guidance**

The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to CMS operations and assets, individuals, other organizations, and the Nation.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AS-2, AS-3; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); HSPD 7: D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-6.1**

**Assessment Objective**

Determine if:

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

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.

**AC-6(1) – Enhancement (High)**

**Control**

The organization explicitly authorizes access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.

**Guidance**

Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-6(1).1**

**Assessment Objective**

Determine if:
the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized;

the organization explicitly authorizes access to the organization-defined security functions and security-relevant information.

**Assessment Methods And Objects**

**Examine:** Access control policy; 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; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.

| AC-6(2) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization requires that users of information system accounts, or roles, with access to administrator accounts or 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. | | |
| **Guidance**<br>This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy such as Role Based Access Control (RBAC) is being implemented 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. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-6(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access;<br>the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions;<br>the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions. | | |
| **Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.<br>**Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. | | |

| AC-7 – Unsuccessful Login Attempts (High) | | |
|---|---|---|
| **Control**<br>The information system:<br>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<br>b. Automatically disables or locks the account/node until released after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.<br>**Implementation Standard(s)**<br>1. Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user during a one (1) hour time period. Require the lock out to persist for a minimum of three (3) hours. | | |
| **Guidance**<br>Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2; IRS-1075: 5.6.3.2#4.1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid login attempts occur;<br>the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period; | | |

the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:
- lock out the account/node for a specified time period;
- lock out the account/note until released by an administrator; or
- delay the next login prompt according to organization-defined delay algorithm;

the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded;

the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing unsuccessful login attempts; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for unsuccessful login attempts.

## AC-8 – System Use Notification (High)

**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 for CMS information systems is:

- You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  * You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information 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 information system.
  * Any communication or data transiting or stored on this information 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: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

**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 CMS 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, web sites, web pages where substantial personal information from the public is collected, ftp, telnet, or other services accessed.

System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2 | **Related Controls Requirement(s):** SI-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-8.1**

**Assessment Objective**

Determine if:

the information system displays the CMS-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 and states that:

- users are accessing a U.S. Government information system;
- system usage may be monitored, recorded, and subject to audit;
- unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- use of the system indicates consent to monitoring and recording;

the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system;

the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for system use notification.

**ASSESSMENT PROCEDURE: AC-8.2**

**Assessment Objective**

Determine if:
the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access;

the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities;

the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for system use notification.

**AC-9 – Previous Logon (Access) Notification (High)**

**Control**

The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access), both successful and unsuccessful.

**Guidance**

This control is intended to cover both traditional logons to information systems and general accesses to information systems that occur in other types of architectural configurations (e.g., service oriented architectures).
Due to the possibility that an unauthorized person may have the ability to log-on to a system or application using an authorized person's log-on account, all CMS systems and applicable applications will provide an automated method of notifying the authorized user of the last successful log-on date and time, and a number of previously unsuccessful log-on attempts. It is important that training include reporting procedures and responsibility for authorized users to report unauthorized log-ons and unauthorized attempts to log-on.

| | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** FISCAM: AC-1 | **Related Controls**<br>**Requirement(s):** AC-7.Std.1, CA-7(1) |

**ASSESSMENT PROCEDURE: AC-9.1**

**Assessment Objective**

Determine if the information system, upon successful user logon (access), displays to the user the date and time of the last logon (access).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing previous logon notification; information system configuration settings and associated documentation; information system notification messages; information system design documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for previous logon notification.

**AC-9(1) – Enhancement (High)**

**Control**

The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

| | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** | **Related Controls**<br>**Requirement(s):** |

| **ASSESSMENT PROCEDURE: AC-9(1).1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if the information system, upon successful user logon/access, displays to the user the number of unsuccessful logon/access attempts since the last successful logon/access.<br>**Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing previous logon notification; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.<br>**Test:** Automated mechanisms implementing the access control policy for previous logon notification. | | |
| **AC-10 – Concurrent Session Control (High)** | | |
| **Control**<br>The information system limits the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan. | | |
| **Guidance**<br>This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.<br>A session is 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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2 | **Related Controls Requirement(s):** |

| **ASSESSMENT PROCEDURE: AC-10.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, the maximum number of concurrent sessions to be allowed for each system account;<br>the information system limits the number of concurrent sessions for each system account to the organization-defined number of sessions.<br>**Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing concurrent session control; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records.<br>**Test:** Automated mechanisms implementing the access control policy for concurrent session control. | | |
| **AC-11 – Session Lock (High)** | | |
| **Control**<br>The information system:<br>a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity; and<br>b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. | | |
| **Guidance**<br>A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AS-2; IRS-1075: 5.6.3.2#4.3 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AC-11.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the time period of user inactivity after which the information system initiates a session lock;

the information system initiates a session lock after the organization-defined time period of inactivity or upon receiving a request from a user;

the information system retains the session lock until the user reestablishes access using established identification and authentication procedures.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for session lock.

**AC-12 – Session Termination (High)**

**Control**

[Withdrawn: Incorporated into SC-10].

**AC-13 – Supervision and Review--Access Control (High)**

**Control**

[Withdrawn: Incorporated into AC-2 and AU-6].

**AC-14 – Permitted Actions without Identification or Authentication (High)**

**Control**

The organization:
a. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication; and
b. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

**Implementation Standard(s)**

1. Identify and document specific user actions that can be performed on the information system without identification or authentication.

**Guidance**

This control is intended for public websites and other publicly available systems. It is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as http://www.usa.gov). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login 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 being repeated, but rather to situations where identification and/or authentication have not yet occurred.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AS-2 | **Related Controls Requirement(s):** IA-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-14.1**

**Assessment Objective**

Determine if:
the organization identifies specific user actions that can be performed on the information system without identification or authentication;

the organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

the organization meets all the requirements specified in the applicable 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; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records.

| AC-14(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish CMS mission/business objectives. | | |
| **Applicability:** All | **Reference(s):** HIPAA: 164.312(c)(1) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-14(1).1** | | |
| **Assessment Objective**<br>Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.<br>**Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records. | | |
| **AC-15 – Automated Marking (High)** | | |
| **Control**<br>[Withdrawn: Incorporated into MP-3]. | | |
| **AC-17 – Remote Access (High)** | | |
| **Control**<br>Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:<br>a. Documents allowed methods of remote access to the information system;<br>b. Establishes usage restrictions and implementation guidance for each allowed remote access method;<br>c. Monitors for unauthorized remote access to the information system;<br>d. Authorizes remote access to the information system prior to connection; and<br>e. Enforces requirements for remote connections to the information system.<br>**Implementation Standard(s)** | | |

1. Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified within every three hundred sixty-five (365) days.
2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix D: E-authentication Standard.

**Guidance**

This control requires explicit authorization prior to allowing remote access to a CMS information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to a CMS information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network (VPN) when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to CMS information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AC-4; IRS-1075: 5.6.3.2#5, 5.7.1#1 | **Related Controls Requirement(s):** IA-2, SC-9 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17.1**

**Assessment Objective**

Determine if:

the organization documents allowed methods of remote access to the information system;

the organization establishes usage restrictions and implementation guidance for each allowed remote access method;

the organization monitors for unauthorized remote access to the information system;

the organization authorizes remote access to the information system prior to connection;

the organization enforces requirements for remote connections to the information system.

the organization meets all the requirements specified in the applicable 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; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with remote access authorization, monitoring, and control responsibilities.

**Test:** Remote access methods for the information system.

**AC-17(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

**Guidance**

Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(1).1**

**Assessment Objective**

Determine if the information system employs automated mechanisms to facilitate the monitoring and control of remote access methods.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for remote access.

**AC-17(2) – Enhancement (High)**

**Control**

The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

**Guidance**

Use only the CMS-approved encryption standard (see SC-13).

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#5, 5.7.1#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(2).1**

**Assessment Objective**

Determine if the organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing cryptographic protections for remote access.

**AC-17(3) – Enhancement (High)**

**Control**

The information system routes all remote accesses through a limited number of managed access control points.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(3).1**

**Assessment Objective**

Determine if:
the organization defines a limited number of managed access control points for remote access to the information system;

the information system routes all remote accesses through managed access control points.

**Assessment Methods And Objects**

**Examine:** Access control policy; 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; other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for remote access.

| AC-17(4) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-17(4).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs;<br>the organization documents the rationale for such access in the security plan for the information system.<br>**Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records. | | |
| **AC-17(5) – Enhancement (High)** | | |
| **Control**<br>The organization monitors for unauthorized remote connections to the information system at least quarterly, and takes appropriate action if an unauthorized connection is discovered. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-17(5).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization monitors for unauthorized remote connections to the information system in accordance with the organization-defined frequency; | | |

the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered;

the organization takes organization-defined appropriate action(s) if an unauthorized connection is discovered.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for monitoring remote connections to the information system.

**AC-17(7) – Enhancement (High)**

**Control**

The organization ensures that remote sessions used for remote administration employ additional security measures (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled) and the CMS-approved encryption standard (see SC-13), and the sessions are audited.

**Guidance**

Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(7).1**

**Assessment Objective**

Determine if:

the organization defines the security functions and security-relevant information that can be accessed using remote sessions;

the organization defines the additional security measures to be employed for remote sessions used to access organization-defined security functions and security-relevant information;

the organization employs the CMS-approved encryption standard (see SC-13) for remote sessions used to access organization-defined security functions and security-relevant information;

the organization audits remote sessions for accessing organization-defined security functions and security-relevant information, if required by the control.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records (if auditing is required); other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for remote access.

**AC-17(8) – Enhancement (High)**

**Control**

The organization disables Bluetooth and peer-to-peer networking protocols within the information system except for explicitly identified components in support of specific operational requirements.

**Guidance**

The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(8).1**

**Assessment Objective**

Determine if the organization disables Bluetooth and peer-to-peer networking protocols within the information system except for explicitly identified components in support of specific operational requirements.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; security plan; list of networking protocols deemed to be non-secure; other relevant documents or records.

**Test:** Automated mechanisms disabling networking protocols deemed to be non-secure.

## AC-18 – Wireless Access (High)

**Control**

The organization prohibits the installation of wireless access points (WAP) to CMS information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If authorized, the organization:
a. Monitors for unauthorized wireless access to the information system; and
b. Enforces requirements for wireless connections to the information system.

**Implementation Standard(s)**

1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented:
(a) Encryption protection is enabled;
(b) Access points are placed in secure areas;
(c) Access points are shut down when not in use (i.e., nights, weekends);
(d) A firewall is implemented between the wireless network and the wired infrastructure;
(e) MAC address authentication is utilized;
(f) Static IP addresses, not DHCP, is utilized;
(g) Personal firewalls are utilized on all wireless clients;
(h) File sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall; and
(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

**Guidance**

Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AC-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-18.1**

**Assessment Objective**

Determine if:
the organization establishes usage restrictions and implementation guidance for wireless access;

the organization monitors for unauthorized wireless access to the information system;

the organization authorizes wireless access to the information system prior to connection;

the organization enforces requirements for wireless connections to the information system.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system.

**Test:** Wireless access usage and restrictions.

**AC-18(1) – Enhancement (High)**

**Control**

If wireless access is explicitly approved, the information system protects wireless access to the system using authentication and encryption.

**Guidance**

Authentication applies to user, device, or both as necessary.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-18(1).1**

**Assessment Objective**

Determine if the information system protects wireless access to the system using authentication and encryption.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Test:** Automated mechanisms implementing the access control policy for wireless access to the information system.

| AC-18(2) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points quarterly, and takes appropriate action if an unauthorized connection is discovered. | | |
| **Guidance**<br>Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-18(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, in accordance with organization-defined frequency;<br>the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered;<br>the organization takes appropriate action(s) if an unauthorized connection discovered. | | |
| **Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records.<br>**Interview:** Organizational personnel responsible for monitoring wireless connections to the information system.<br>**Test:** Scanning procedures for detecting unauthorized wireless connections and access points. | | |
| **AC-18(4) – Enhancement (High)** | | |
| **Control**<br>The organization does not allow users to independently configure wireless networking capabilities. | | |

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-18(4).1**

**Assessment Objective**

Determine if the organization does not allow users to independently configure wireless networking capabilities.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Test:** Automated mechanisms preventing independent configuration of wireless networking capabilities.

**AC-18(5) – Enhancement (High)**

**Control**

The organization confines wireless communications to organization-controlled boundaries.

**Guidance**

Actions that may be taken by the organization to confine wireless communications to organization-controlled boundaries include: (i) reducing the power of the wireless transmission such that it cannot transit the physical perimeter of the organization; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) configuring the wireless access such that it is point to point in nature.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-18(5).1**

**Assessment Objective**

Determine if the organization confines wireless communications to organization-controlled boundaries.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**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)**

**Control**

The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants [PDA], cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;
b. Monitors for unauthorized connections of mobile devices to CMS information systems;
c. Enforces requirements for the connection of mobile devices to CMS information systems;
d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

**Guidance**

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to 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). Examples of information system functionality that provide the capability for automatic execution of code are Auto-Run and Auto-Play. Organizational policies and procedures for mobile devices 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 measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures 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 family.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1; IRS-1075: 4.6#1 | **Related Controls Requirement(s):** MP-4, MP-5 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-19.1**

**Assessment Objective**

Determine if:

the organization prohibits the connection of portable and mobile devices to the information system unless explicitly authorized, in writing, by the CIO;

if authorized, the organization employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;

if authorized, the organization monitors for unauthorized connections of mobile devices to organizational information systems;

if authorized, the organization enforces requirements for the connection of mobile devices to organizational information systems;

if authorized, the organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

if authorized, the organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures;

if authorized, the organization defines the inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be of significant risk;

if authorized, the organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

**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; other relevant documents or records.

**Interview:** Organizational personnel who use portable and mobile devices to access the information system.

**Test:** Automated mechanisms implementing access control policy for portable and mobile devices.

**AC-19(1) – Enhancement (High)**

**Control**

The organization restricts the use of writable, removable media in CMS information systems.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-19(1).1**

**Assessment Objective**

Determine if the organization restricts the use of writable, removable media in organizational information systems.

**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; other relevant documents or records.

**Interview:** Organizational personnel who use portable and mobile devices to access the information system.

**Test:** Automated mechanisms implementing access control policy for portable and mobile devices.

**AC-19(2) – Enhancement (High)**

**Control**

The organization prohibits the use of personally owned, removable media in CMS information systems.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-19(2).1**

**Assessment Objective**

Determine if the organization prohibits the use of personally owned, removable media in organizational information systems.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing access control policy for portable and mobile devices.

**AC-19(3) – Enhancement (High)**

**Control**

The organization prohibits the use of removable media in CMS information systems when the media has no identifiable owner.

**Guidance**

An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-19(3).1**

**Assessment Objective**

Determine if the organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing access control policy for portable and mobile devices.

**AC-20 – Use of External Information Systems (High)**

**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 CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall 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 virtual private networking (VPN) and 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 Standard(s)**

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.
2. (For PII only) Only organization owned computers and software can be used to process, access, and store PII.

**Guidance**

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular 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. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies.

This control does not apply to the use of external information systems to access public interfaces to CMS information systems and information (e.g., individuals accessing federal information through www.medicare.gov). The organization establishes terms and conditions for the use of external information systems in accordance with CMS security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the CMS information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17.

| **Applicability:** All | **Reference(s):** FISCAM: SM-7; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-20.1**

**Assessment Objective**

Determine if:

the organization prohibits the use of external information systems to store, access, transmit, or process sensitive information unless explicitly authorized, in writing, by the CIO;

if authorized, the organization identifies individuals authorized to:
- access the information system from the external information systems;
- process, store, and/or transmit organization-controlled information using the external information systems;

if authorized, the terms and conditions address, at a minimum:
- the types of applications that can be accessed from external information systems;
- the maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
- how other users of the external information system will be prevented from accessing federal information;
- the use of virtual private networking (VPN) and firewall technologies;
- the use of and protection against the vulnerabilities of wireless technologies;
- the maintenance of adequate physical security controls;
- the use of virus and spyware protection software; and
- how often the security capabilities of installed software are to be updated.

the organization meets all the requirements specified in the applicable implementation standard(s).

only organizational owned computers and software are used to process, access, and store PII.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems.

**AC-20(1) – Enhancement (High)**

**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) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

| **Applicability:** All | **Reference(s):** IRS-1075: 4.7.2#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-20(1).1**

**Assessment Objective**

Determine if 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:
- can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
- has approved information system connection or processing agreements with the organizational entity hosting the external information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing the use of external information systems; security plan; information system connection or processing agreements; account management documents; other relevant documents or records.

**AC-20(2) – Enhancement (High)**

**Control**

The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

**Guidance**

Limits on the use of organization-controlled portable storage media in external information systems can 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.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-20(2).1**

**Assessment Objective**

Determine if the organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing the use of external information systems; security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records.

**AC-22 – Publicly Accessible Content (High)**

**Control**

The organization:
a. Designates individuals authorized to post information onto a CMS information system that is publicly accessible;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the CMS information system;
d. Reviews the content on the publicly accessible CMS information system for nonpublic information monthly; and
e. Removes nonpublic information from the publicly accessible CMS information system, if discovered.

**Guidance**

Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on a CMS information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-CMS information systems is covered by appropriate organizational policy.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-22.1**

**Assessment Objective**

Determine if:
the organization designates individuals authorized to post information onto a CMS information system that is publicly accessible;

the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the CMS information system;

the organization reviews the content on the publicly accessible CMS information system for nonpublic information monthly;

the organization removes nonpublic information from the publicly accessible CMS information system, if discovered.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records; other relevant documents or records.

**Interview:** Organizational personnel responsible for managing publicly accessible information posted on organizational information systems.

# 2.0AWARENESS AND TRAINING (AT) – OPERATIONAL

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **AT-1 – Security Awareness and Training Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular CMS information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SM-1, SM-3, SM-7; IRS-1075: 5.6.2.7#1.1-2, 6.1#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AT-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security awareness and training policy; | | |

the organization security awareness and training policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities, and compliance;

the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities;

the organization develops and formally documents security awareness and training procedures;

the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls;

the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities;

the organization reviews/updates the security awareness and training policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with security awareness and training responsibilities.

**AT-2 – Security Awareness (High)**

**Control**

The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by system changes, and within every three hundred sixty-five (365) days thereafter.

**Guidance**

The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the CMS information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to CMS' information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SM-4; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AT-2.1**

**Assessment Objective**

Determine if:

the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually;

the organization provides refresher security awareness training in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records.

**Interview:** Organizational personnel comprising the general information system user community.

**AT-3 – Security Training (High)**

**Control**

The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) refresher training within every three hundred sixty-five (365) days thereafter.

**Implementation Standard(s)**

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 system changes; and refresher training within every three hundred sixty-five (365) days thereafter.

**Guidance**

The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of CMS and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of CMS' information security program.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-4; IRS-1075: 5.6.2.7#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AT-3.1**

**Assessment Objective**

Determine if:
the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes;

the organization provides role-based security-related refresher training within every three hundred sixty-five (365) days thereafter.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for role-based, security-related training; organizational personnel with significant information system security responsibilities.

| AT-4 – Security Training Records (High) |
| --- |
| **Control**<br>The organization:<br>a. Documents and monitors individual CMS information system security training activities including basic security awareness training and specific information system security training; and<br>b. Retains individual training records for three (3) years. |

**Guidance**

Procedures and training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
1) All users of CMS information systems must be exposed to security awareness materials at least annually. 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 basics and policy level training in security planning and management.
3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) 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.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-4; IRS-1075: 6.2#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

| ASSESSMENT PROCEDURE: AT-4.1 | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training;<br>the organization retains individual training records in accordance with the organization-defined time period.<br>**Assessment Methods And Objects**<br>**Examine:** Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.<br>**Interview:** Organizational personnel with security training record retention responsibilities. | | |
| **AT-5 – Contacts with Security Groups and Associations (High)** | | |
| **Control**<br>The organization establishes and institutionalizes contact with selected groups and associations within the security community:<br>- To facilitate ongoing security education and training for organizational personnel;<br>- To stay up to date with the latest recommended security practices, techniques, and technologies; and<br>- To share current security-related information including threats, vulnerabilities, and incidents. | | |
| **Guidance**<br>Ongoing contact with security groups and associations is of paramount importance in an environment of rapid technology changes and dynamic threats. Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Information-sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5; HSPD 7: H(25) | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AT-5.1**

**Assessment Objective**

Determine if the organization establishes and institutionalizes contact with selected groups and associations within the security community:
- to facilitate ongoing security education and training for organizational personnel;
- to stay up to date with the latest recommended security practices, techniques, and technologies;
- to share current security-related information including threats, vulnerabilities, and incidents.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records.

**Interview:** Organizational personnel with security responsibilities (e.g., individuals that have contacts with selected groups and associations within the security community).

# 3.0AUDIT AND ACCOUNTABILITY (AU) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **AU-1 – Audit and Accountability Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular CMS information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, SM-1, SM-3; IRS-1075: 5.6.3.3#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents audit and accountability policy; | | |

the organization audit and accountability policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities;

the organization develops and formally documents audit and accountability procedures;

the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls;

the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities.

the organization reviews/updates the audit and accountability policy and procedures within every three hundred sixty-five (365) days.

**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 – Auditable Events (High)**

**Control**

The organization:
a. Determines, based on a risk assessment and CMS mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
c. Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

**Implementation Standard(s)**

1. Generate audit records for the following events:
(a) User account management activities,
(b) System shutdown,
(c) System reboot,
(d) System errors,
(e) Application shutdown,
(f) Application restart,
(g) Application errors,
(h) File creation,
(i) File deletion,
(j) File modification,
(k) Failed and successful log-ons,
(l) Security policy modifications,
(m) Use of administrator privileges, and
(n) File access.
2. Enable logging for perimeter devices, including firewalls and routers.
(a) Log packet screening denials originating from un-trusted networks,
(b) Packet screening denials originating from trusted networks,
(c) User account management,
(d) Modification of packet filters,
(e) Application errors,
(f) System shutdown and reboot,
(g) System errors, and
(h) Modification of proxy services.
3. Verify that proper logging is enabled in order to audit administrator activities.
4. (For FTI only) Generate audit records for the following events in addition to those specified in other controls:
(a) All successful and unsuccessful authorization attempts.
(b) All changes to logical access control authorities (e.g., rights, permissions).
(c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
(d) The audit trail shall capture the enabling or disabling of audit report generation services.
(e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

**Guidance**

The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system 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 extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AC-5, AS-2, DA-1; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1 | **Related Controls Requirement(s):** AU-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-2.1**

**Assessment Objective**

Determine if:

the organization determines, based on a risk assessment and CMS mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;

the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events;

the organization provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;

the organization defines in the security plan, explicitly or by reference, information system auditable events;

the organization defines the subset of auditable events defined in (a) that are to be audited within the information system and (b) the frequency of (or situation requiring) auditing for each identified event;

the organization determines, based on current threat information and ongoing assessment of risk, the subset of auditable events defined in (a) to be audited within the information system, and (b) the frequency of (or situation requiring) auditing for each identified event.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records.

**Interview:** Organizational personnel with auditing and accountability responsibilities.

**Test:** Automated mechanisms implementing information system auditing of organization-defined auditable events.

**AU-2(1) – Enhancement (High)**

**Control**

[Withdrawn: Incorporated into AU-12].

**AU-2(2) – Enhancement (High)**

**Control**

[Withdrawn: Incorporated into AU-12].

**AU-2(3) – Enhancement (High)**

**Control**

The organization reviews and updates the list of auditable events within every three hundred sixty-five (365) days.

**Guidance**

The list of auditable events is defined in AU-2.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.3#2.1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-2(3).1**

**Assessment Objective**

Determine if the organization reviews and updates the list of organization-defined auditable events in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing auditable events; security plan; list of organization-defined auditable events; auditable events review and update records; information system audit records; information system incident reports; other relevant documents or records.

**Interview:** Organizational personnel with auditing and accountability responsibilities.

| AU-2(4) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization includes execution of privileged functions in the list of events to be audited by the information system, including administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-2(4).1** | | |
| **Assessment Objective**<br>Determine if the organization includes execution of privileged functions in the list of events to be audited by the information system.<br>**Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing auditable events; information system configuration settings and associated documentation; list of organization-defined auditable events; list of privileged security functions; other relevant documents or records. | | |
| **AU-3 – Content of Audit Records (High)** | | |
| **Control**<br>The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.<br>**Implementation Standard(s)**<br>1. (For PHI only) 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. | | |
| **Guidance**<br>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. | | |

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-2, DA-1; IRS-1075: 5.6.3.3#3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-3.1**

**Assessment Objective**

Determine if:
the information system produces audit records that contain sufficient information to, at a minimum, establish:
- what type of event occurred;
- when (date and time) the event occurred;
- where the event occurred;
- the source of the event;
- the outcome (success or failure) of the event;
- the identity of any user/subject associated with the event.

-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; other relevant documents or records.

**Test:** Automated mechanisms implementing information system auditing of auditable events.

**AU-3(1) – Enhancement (High)**

**Control**

The information system includes the capability to include more detailed information in the audit records for audit events identified by type, location, or subject.

**Guidance**

An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-3(1).1**

**Assessment Objective**

Determine if:
the organization defines the additional, more detailed information to be included in audit records for audit events identified by type, location, or subject;

the information system includes the organization-defined additional, more detailed information in the audit records for audit events identified by type, location, or subject.

**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; security plan; information system configuration settings and associated documentation; other relevant documents or records.

**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) – Enhancement (High)**

**Control**

The organization centrally manages the content of audit records generated by individual components through out the information system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-3(2).1**

**Assessment Objective**

Determine if:
the organization defines the information system components for which the content of audit records generated is centrally managed;

the organization centrally manages the content of audit records generated by organization-defined information system components.

**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.

**Test:** Automated mechanisms implementing centralized management of audit record content.

**AU-4 – Audit Storage Capacity (High)**

**Control**

The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

**Guidance**

The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.3.3#4 | **Related Controls Requirement(s):** AU-2, AU-5, AU-6, AU-7, SI-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-4.1**

**Assessment Objective**

Determine if:
the organization allocates audit record storage capacity;

the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Test:** Audit record storage capacity and related configuration settings.

| AU-5 – Response to Audit Processing Failures (High) | | |
|---|---|---|
| **Control**<br>The information system:<br>a. Alerts designated organizational officials in the event of an audit processing failure; and<br>b. Takes the following additional actions in response to an audit failure or audit storage capacity issue:<br>- Shutdown the information system,<br>- Stop generating audit records, or<br>- Overwrite the oldest records, in the case that storage media is unavailable. | | |
| **Guidance**<br>Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5, DA-1 | **Related Controls Requirement(s):** AU-4 |
| **ASSESSMENT PROCEDURE: AU-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines designated organizational officials to be alerted in the event of an audit processing failure;<br>the organization defines in the security plan, explicitly or by reference, personnel to be notified in case of an audit processing failure;<br>the organization defines additional actions to be taken in the event of an audit processing failure;<br>the information system takes the additional organization-defined actions in the event of an audit processing failure. | | |
| **Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.<br>**Test:** Automated mechanisms implementing information system response to audit processing failures. | | |

| AU-5(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The information system provides a warning when allocated audit record storage volume reaches 80% of maximum audit record storage capacity. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-5(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the percentage of maximum audit record storage capacity that, if reached, requires a warning to be provided;<br>the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.<br>**Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.<br>**Test:** Automated mechanisms implementing audit storage limit warnings. | | |
| **AU-5(2) – Enhancement (High)** | | |
| **Control**<br>The information system provides a real-time alert when the audit record log is full. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-5(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines audit failure events requiring real-time alerts;<br>the information system provides a real-time alert when organization-defined audit failure events occur. | | |

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Test:** Automated mechanisms implementing real time audit alerts when organization-defined audit failure events occur.

**AU-6 – Audit Review, Analysis, and Reporting (High)**

**Control**

The organization:
a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity, and report findings to designated organizational officials; and
b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

**Implementation Standard(s)**

1. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment.
2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment.
3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
4. Use automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.
5. Inspect administrator groups on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.
6. Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.
7. (For FTI only) All requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log. (see IRS Pub. 1075, sect 6.3.1)

**Guidance**

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to CMS operations, CMS assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AC-5, AS-2, DA-1, SM-5; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1 | **Related Controls Requirement(s):** AU-4, IR-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-6.1**

**Assessment Objective**

Determine if:

the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency;

the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

the organization report findings of inappropriate/unusual activities, to designated organizational officials.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** Logs for requests of FTI include receipt and/or disposal or FTI information is returned.

**Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities.

**Interview:** Organizational personnel responsible for handling FTI.

**Test:** Information system audit review, analysis, and reporting capability.

**ASSESSMENT PROCEDURE: AU-6.2**

**Assessment Objective**

Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit review, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities.

**AU-6(1) – Enhancement (High)**

**Control**

The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

| **Applicability:** All | **Reference(s):** HIPAA: 164.312(b) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-6(1).1**

**Assessment Objective**

Determine if the information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

**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; other relevant documents or records.

**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(2) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>[Withdrawn: Incorporated into SI-4]. | | |
| **AU-7 – Audit Reduction and Report Generation (High)** | | |
| **Control**<br>The information system provides an audit reduction and report generation capability. | | |
| **Guidance**<br>An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** AU-4 |
| **ASSESSMENT PROCEDURE: AU-7.1** | | |
| **Assessment Objective**<br>Determine if the information system provides an audit reduction and report generation capability.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities.<br>**Test:** Audit reduction and report generation capability. | | |
| **AU-7(1) – Enhancement (High)** | | |
| **Control**<br>The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AU-7(1).1**

**Assessment Objective**

Determine if the information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

**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; other relevant documents or records.

**Test:** Audit reduction and report generation capability.

**AU-8 – Time Stamps (High)**

**Control**

The information system uses internal system clocks to generate time stamps for audit records.

**Guidance**

Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-8.1**

**Assessment Objective**

Determine if the information system uses internal system clocks to generate time stamps for audit records.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Test:** Automated mechanisms implementing time stamp generation.

| AU-8(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The information system synchronizes internal information system clocks daily and at system boot. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-8(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, the frequency of internal clock synchronization for the information system;<br>the organization defines the authoritative time source for internal clock synchronization;<br>the organization synchronizes internal information system clocks with the organization-defined authoritative time source in accordance with the organization-defined frequency.<br>**Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing time stamp generation; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.<br>**Test:** Automated mechanisms implementing internal information system clock synchronization. | | |
| **AU-9 – Protection of Audit Information (High)** | | |
| **Control**<br>The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | | |
| **Guidance**<br>Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AU-9.1**

**Assessment Objective**

Determine if the information system protects audit information and audit tools from unauthorized:
- access;
- modification;
- deletion;

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing audit information protection.

**AU-10 – Non-Repudiation (High)**

**Control**

The information system protects against an individual falsely denying having performed a particular action.

**Guidance**

Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. 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. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-10.1**

**Assessment Objective**

Determine if the information system protects against an individual falsely denying having performed a particular action.

**Assessment Methods And Objects**

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

**Test:** Automated mechanisms implementing non-repudiation capability.

**AU-11 – Audit Record Retention (High)**

**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 Standard(s)**

1. (For FTI only) Employ a permanent system of standardized records of request for disclosure of FTI and maintain the records for five (5) years or the applicable records control schedule, whichever is longer.
2. (For FTI only) To support the audit of FTI activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored.
3. (For PII only) Audit inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.

**Guidance**

The organization retains 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. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-11.1**

**Assessment Objective**

Determine if:

the retention period for audit records is consistent with the records retention policy;

the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

the organization employs mechanisms to facilitate the review of PII disclosures/access records and retains the records for five (5) years or the applicable records control schedule, whichever is longer;

the organization ensures that audit information is archived for six (6) years to enable the recreation of computer related accesses to both the operation system and the application wherever PII is stored;

the organizational PII inspection reports include a record of corrective actions, which is retained for a minimum of three (3) years from the date the inspection was completed.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

**Examine:** PII disclosure/access audit records; PII audit information; PII inspection records; other relevant documents or records.

**Interview:** Organizational personnel with information system audit record retention responsibilities.

| AU-12 – Audit Generation (High) | | |
|---|---|---|
| **Control**<br>The information system:<br>a. Provides audit record generation capability for the following events in addition to those specified in other controls:<br>- All successful and unsuccessful authorization attempts.<br>- All changes to logical access control authorities (e.g., rights, permissions).<br>- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.<br>- The audit trail shall capture the enabling or disabling of audit report generation services.<br>- The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).<br>b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and<br>c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. | | |
| **Guidance**<br>Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-12.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2;<br>the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2;<br>the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; | | |

the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system audit record generation responsibilities.

**Test:** Automated mechanisms implementing audit record generation capability.

**AU-12(1) – Enhancement (High)**

**Control**

The information system compiles audit records from multiple components throughout the system into a system-wide (logical or physical) time-correlated audit trail.

**Guidance**

The audit trail is 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.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-12(1).1**

**Assessment Objective**

Determine if:

the information system produces a system-wide (logical or physical) audit trail of information system audit records;

the organization defines the information system components from which audit records are to be compiled into the system-wide audit trail;

the information system compiles audit records from organization-defined information system components into the system-wide audit trail;

the organization defines the acceptable level of tolerance for relationship between time stamps of individual records in the system-wide audit trail;

the system-wide audit trail is time-correlated to within the organization-defined level of tolerance to achieve a time ordering of audit records.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing audit record generation capability.

# 4.0SECURITY ASSESSMENT AND AUTHORIZATION (CA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CA-1 – Security Assessment and Authorization Policies and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security assessment and authorization family [formerly called Certification and Accreditation [C&A] family and process). The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 5.6.1.4#1.1-2 | **Related Controls Requirement(s):** CA-6 |
| **ASSESSMENT PROCEDURE: CA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security assessment and authorization policy; | | |

the organization security assessment and authorization policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities;

the organization develops and formally documents security assessment and authorization procedures;

the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls;

the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities;

the organization reviews/updates the security assessment and authorization policies and procedures within every three hundred sixty-five (365) days;

**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)

**Control**

The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system 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 the security requirements for the system;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

**Implementation Standard(s)**

1. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems.
2. The annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset (no less than one-third [1/3]) of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period.
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, ISSO).

**Guidance**

The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by CMS, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the FISMA annual assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring. The organization establishes 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 provided that the results are current, valid, and relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-3, SM-5; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1 | **Related Controls**<br>**Requirement(s):** CA-4, CA-6, CA-7, CA-7(1), CA-7(2), SA-11, SI-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-2.1**

**Assessment Objective**

Determine if:
the organization develops a security assessment plan for the information system;

the security assessment plan describes the scope of the assessment including:
- security controls and control enhancements under assessment;
- assessment procedures to be used to determine security control effectiveness;
- assessment environment, assessment team, and assessment roles and responsibilities;

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Security assessment policy; procedures addressing security assessments; security plan; security assessment plan; assessment evidence; other relevant documents or records.

**ASSESSMENT PROCEDURE: CA-2.2**

**Assessment Objective**

Determine if:
the organization assesses the security controls in the information system within every three hundred sixty-five (365) days in accordance with the CMS IS ARS Including 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 the security requirements for the system;

the organization provides the results of the security control assessment within every 365 days, in writing, to the Business Owner;

the Business Owner reviews the assessment documentation and updates system security documentation where necessary to reflect any changes to the system;

the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records.

**Interview:** Organizational personnel with security assessment responsibilities.

## CA-2(1) – Enhancement (High)

**Control**

The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

**Guidance**

An independent assessor or assessment team is any individual or group capable of conducting an impartial assessment of a CMS information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, accuracy, integrity, and reliability of the results.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: CA-2(1).1

**Assessment Objective**

Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

**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); other relevant documents or records.

**Interview:** Organizational personnel with security assessment responsibilities.

| CA-2(2) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization includes as part of security control assessments, within every three hundred sixty-five (365) days, announced or unannounced in-depth system monitoring and malicious user testing. | | |
| **Guidance**<br>Information system monitoring, malicious user testing, penetration testing, red-team exercises, and other forms of security testing (e.g., independent verification and validation) are conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization. Testing is conducted in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Testing methods are approved by authorizing officials in coordination with the organization's Risk Executive Function. Vulnerabilities uncovered during red team exercises are incorporated into the vulnerability remediation process. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CA-2(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines:<br>- the forms of security testing to be included in security control assessments, selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing;<br>- the frequency for conducting each form of security testing;<br>- whether the security testing will be announced or unannounced;<br>the organization conducts security control assessments using organization-defined forms of testing in accordance with organization-defined frequency and assessment techniques established for each form of testing. | | |
| **Assessment Methods And Objects**<br>**Examine:** Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records.<br>**Interview:** Organizational personnel with security assessment responsibilities. | | |

| CA-3 – Information System Connections (High) |
|---|
| **Control**<br>The organization:<br>a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;<br>b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and<br>c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.<br>**Implementation Standard(s)**<br>1. Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location. |
| **Guidance**<br>This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between CMS and a nonfederal (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, SM-1; HSPD 7: F(19) | **Related Controls Requirement(s):** SA-9, SC-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-3.1**

**Assessment Objective**

Determine if:
the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);

the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;

the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated;

the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements;

the organization meets all the requirements specified in the applicable 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; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records.

**Interview:** Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements.

**CA-4 – Security Certification (High)**

**Control**

[Withdrawn: Incorporated into CA-2].

| CA-5 – Plan of Action and Milestones (POA&M) (High) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Develops and submits a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and<br>b. Updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. | | |
| **Guidance**<br>The POA&M is a key document in the security authorization package and is subject to federal reporting requirements established by OMB. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-5, SM-6; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4 | **Related Controls Requirement(s):** CA-7 |
| **ASSESSMENT PROCEDURE: CA-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops a plan of action and milestones for the information system within thirty (30) days of the final results for every internal/external audit/review or test;<br>the plan of action and milestones documents 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;<br>the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates;<br>the organization updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. | | |
| **Assessment Methods And Objects**<br>**Examine:** Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records. | | |

**Interview:** Organizational personnel with plan of action and milestones development and implementation responsibilities.

**CA-5(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-5(1).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is:
- accurate;
- up to date;
- readily available;

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; plan of action and milestones; other relevant documents or records.

**Interview:** Organizational personnel with plan of action and milestones development and implementation responsibilities.

**Test:** Automated mechanisms for developing, implementing and maintaining plan of action and milestones.

| CA-6 – Security Authorization (High) |
| --- |
| **Control**<br>The organization updates the security authorization:<br>- At least every three (3) years;<br>- When substantial changes are made to the system;<br>- When changes in requirements result in the need to process data of a higher sensitivity;<br>- When changes occur to authorizing legislation or federal requirements;<br>- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and<br>- Prior to expiration of a previous security authorization. |
| **Guidance**<br>Security authorization is the official management decision, conveyed through the authorization decision document, given by the CMS CIO or his/her designated representative (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to CMS operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of 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.<br>Through the security authorization process, the CMS CIO is accountable for the security risks associated with CMS information system operations. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the CMS CIO and the applicable information system Business Owner with an up-to-date status of the security state of the information system.<br>To reduce the administrative cost of security reauthorization, the CMS CIO uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. OMB policy requires that federal information systems are reauthorized at least every three years or when there is a significant change to the system.<br>A significant change to the information system includes a physical, administrative, or technical modification that alters the degree of protection required. Examples include, but are not limited to, changes in operating systems, computer hardware, firmware, operational environment, or system boundaries; new services or applications; or other conditions that potentially impact the system's security posture or authorization status. |

| **Applicability:** All | **Reference(s):** FISCAM: SM-2, SM-5; HSPD 7: F(19) | **Related Controls**<br>**Requirement(s):** CA-1, CA-2, CA-4, CA-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-6.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the frequency of authorization updates, not to exceed three years;

the organization updates the security authorization:
- at least every three (3) years;
- when substantial 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;
- 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;

a senior organizational official signs and approves the security authorization package;

**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); other relevant documents or records.

**Interview:** Organizational personnel with security authorization responsibilities.

| CA-7 – Continuous Monitoring (High) | | |
|---|---|---|
| **Control**<br>The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:<br>a. A configuration management process for the information system and its constituent components;<br>b. A determination of the security impact of changes to the information system and environment of operation;<br>c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and<br>d. Reporting the security state of the information system to appropriate organizational officials within every three hundred sixty-five (365) days. | | |
| **Guidance**<br>A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-5; HSPD 7: F(19) | **Related Controls**<br>**Requirement(s):** CA-2, CA-4, CA-5, CA-6, CM-4, SI-2 |
| **ASSESSMENT PROCEDURE: CA-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization establishes a continuous monitoring strategy and program;<br>the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials;<br>the organization defines organizational officials to whom the security state of the information system should be reported; | | |

the organization implements a continuous monitoring program that includes:
- a configuration management process for the information system and its constituent components;
- a determination of the security impact of changes to the information system and environment of operation;
- ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records.

**Interview:** Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities.

**CA-7(1) – Enhancement (High)**

**Control**

The use of independent security assessment agents or teams to monitor security controls is not required. However, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.

**Guidance**

The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's three-year authorization cycle. See supplemental guidance for CA-2, enhancement (1), for further information on assessor independence.

| **Applicability:** All | **Reference(s):** HSPD 7: F(19) | **Related Controls**<br>**Requirement(s):** AC-9, CA-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-7(1).1**

**Assessment Objective**

Determine if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

**Interview:** Organizational personnel with continuous monitoring responsibilities.

## CA-7(2) – Enhancement (High)

**Control**

CMS plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all CMS information systems and information systems that are processing data on behalf of or directly for CMS including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures.

**Guidance**

Examples of vulnerability mitigation procedures are contained in Information Assurance Vulnerability Alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing could also provide evidence of independent validation. See supplemental guidance for CA-2, enhancement (2) for further information on malicious user testing, penetration testing, and other forms of security testing.

| **Applicability:** All | **Reference(s):** | **Related Controls**<br>**Requirement(s):** CA-2 |
|---|---|---|

### ASSESSMENT PROCEDURE: CA-7(2).1

**Assessment Objective**

Determine if:
the organization defines:
- the forms of security testing to be included in planning, scheduling, and security control assessments selecting from in-depth monitoring, malicious user testing, penetration testing, or an organization-defined form of security testing to ensure compliance with all vulnerability mitigation procedures;
- the frequency for conducting each form of security testing;
- whether the security testing will be announced or unannounced;

the organization plans, schedules, and conducts assessments using organization-defined forms of security testing in accordance with the organization-defined frequency and assessment techniques established for each form of testing to ensure compliance with all vulnerability mitigation procedures.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing vulnerability mitigation; 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.

# 5.0CONFIGURATION MANAGEMENT (CM) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CM-1 – Configuration Management Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-1, CP-2, SM-1, SM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents configuration management policy; | | |

the organization configuration management policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities;

the organization develops and formally documents configuration management procedures;

the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls;

the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities;

the organization reviews/updates the configuration management policy and procedures within every three hundred sixty-five (365) days.

**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)**

**Control**

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

**Guidance**

This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of a CMS information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with CMS' enterprise architecture.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2.1**

**Assessment Objective**

Determine if:
the organization develops and documents a baseline configuration of the information system;
the organization maintains, under configuration control, a current baseline configuration of the information system.
the organization documents deviations from the baseline configuration, in support of mission needs/objectives.

**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; other relevant documents or records.

**CM-2(1) – Enhancement (High)**

**Control**

The organization reviews and updates the baseline configuration of the information system:
(a) At least once every three hundred sixty-five (365) days;
(b) When required due to major system changes/upgrades; and
(c) As an integral part of information system component installations and upgrades.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2(1).1**

**Assessment Objective**

Determine if:
the organization defines:
- the frequency of reviews and updates to the baseline configuration of the information system;
- the circumstances that require reviews and updates to the baseline configuration of the information system;

the organization reviews and updates the baseline configuration of the information system:
- in accordance with the organization-defined frequency;
- when required due to organization-defined circumstances;
- as an integral part of information system component installations and upgrades.

**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; other relevant documents or records.

**Interview:** Organizational personnel with configuration change control responsibilities.

**CM-2(2) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

**Guidance**

Software inventory tools are examples of automated mechanisms that help organizations maintain consistent baseline configurations for information systems. Software inventory tools can be deployed for each operating system in use within the organization (e.g., on workstations, servers, network components, mobile devices) and used to track operating system version numbers, applications and types of software installed on the operating systems, and current patch levels. Software inventory tools can also scan information systems for unauthorized software to validate organization-defined lists of authorized and unauthorized software programs.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2(2).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing baseline configuration maintenance.

**CM-2(3) – Enhancement (High)**

**Control**

The organization retains older versions of baseline configurations as deemed necessary to support rollback.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2(3).1**

**Assessment Objective**

Determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback.

**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; other relevant documents or records.

**CM-2(4) – Enhancement (High)**

**Control**

The organization:
(a) Develops and maintains a list of software programs authorized (white list) or unauthorized (black list) to execute on the information system; and
(b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2(4).1**

**Assessment Objective**

Determine if:
the organization develops and maintains a list of software programs not authorized to execute on the information system;

the organization employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software programs not authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records.

**CM-2(5) – Enhancement (High)**

**Control**

The organization:
(a) Develops and maintains a list of software programs authorized (white list) or unauthorized (black list) to execute on the information system; and
(b) Employs a deny-all, permit-by-exception or allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2(5).1**

**Assessment Objective**

Determine if:
the organization develops and maintains a list of software programs authorized to execute on the information system;

the organization employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records.

**CM-2(6) – Enhancement (High)**

**Control**

The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2(6).1**

**Assessment Objective**

Determine if the organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing baseline configuration environments.

| CM-3 – Configuration Change Control (High) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Determines the types of changes to the information system that are configuration controlled;<br>b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;<br>c. Documents approved configuration-controlled changes to the system;<br>d. Retains and reviews records of configuration-controlled changes to the system;<br>e. Audits activities associated with configuration-controlled changes to the system; and<br>f. 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 which meets 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. | | |
| **Guidance**<br>The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-3, BP-2, CM-3, CM-5, CM-6, CP-2; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** CM-4, CM-6, SI-2 |
| **ASSESSMENT PROCEDURE: CM-3.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization determines the types of changes to the information system that are configuration controlled;<br>the organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses; | | |

the organization documents approved configuration-controlled changes to the system;

the organization retains and reviews records of configuration-controlled changes to the system;

the organization audits activities associated with configuration-controlled changes to the system;

the organization defines:
- the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities;
- the frequency with which the configuration change control element convenes, and/or;
- configuration change conditions that prompt the configuration change control element to convene;

the organization 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 which meets 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.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with configuration change control responsibilities.

**CM-3(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to:
(a) Document proposed changes to the information system;
(b) Notify designated approval authorities;
(c) Highlight approvals that have not been received in a timely manner;
(d) Inhibit change until designated approvals are received; and
(e) Document completed changes to the information system.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-3(1).1**

**Assessment Objective**

Determine if:
the organization defines the time period after which approvals that have not been received for proposed changes to the information system are highlighted;

the organization employs automated mechanisms to:
- document proposed changes to the information system;
- notify designated approval authorities;
- highlight approvals that have not been received by the organization-defined time period;
- inhibit change until designated approvals are received;
- document completed changes to the information system.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing configuration change control.

**CM-3(2) – Enhancement (High)**

**Control**

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

**Guidance**

The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the CMS information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|
| **ASSESSMENT PROCEDURE: CM-3(2).1** | | |
| **Assessment Objective**<br>Determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Interview:** Organizational personnel with configuration change control responsibilities. | | |
| **CM-4 – Security Impact Analysis (High)** | | |
| **Control**<br>The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system are audited. | | |
| **Guidance**<br>Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-3, CM-3, CM-4, SM-5 | **Related Controls Requirement(s):** CA-7, CM-3 |

**ASSESSMENT PROCEDURE: CM-4.1**

**Assessment Objective**

Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

**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 architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.

**CM-4(1) – Enhancement (High)**

**Control**

The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-4(1).1**

**Assessment Objective**

Determine if:
the organization analyzes new software in a separate test environment before installation in an operational environment;

the organization, when analyzing new software in a separate test environment, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

**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; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.

**CM-4(2) – Enhancement (High)**

**Control**

The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

**Guidance**

Changes include information system upgrades and modifications.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-4(2).1**

**Assessment Objective**

Determine if the organization, after the information system is changed, checks the security functions to verify that the functions are:
- implemented correctly;
- operating as intended;
- producing the desired outcome with regard to meeting the security requirements for the system.

**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; 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)**

**Control**

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.

**Guidance**

Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of 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 are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AS-3, CM-3, CM-4; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-5.1**

**Assessment Objective**

Determine if:

the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

the organization generates, reviews, and retains records reflecting all such changes.

**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; 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) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-5(1).1** | | |
| **Assessment Objective**<br>Determine if the organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Test:** Automated mechanisms implementing access restrictions for changes to the information system. | | |
| **CM-5(2) – Enhancement (High)** | | |
| **Control**<br>The organization conducts audits of information system changes quarterly and when indications so warrant to determine whether unauthorized changes have occurred. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-5(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the frequency for conducting audits of information system changes;<br>the organization conducts audits of information system changes in accordance with the organization-defined frequency and when indications so warrant to determine whether unauthorized changes have occurred. | | |

**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; security plan; change control records; information system audit records; other relevant documents or records.

**CM-5(3) – Enhancement (High)**

**Control**

The information system prevents the installation of network and operating system software programs that are not signed with a certificate that is recognized and approved by the organization.

**Guidance**

Critical software programs and/or modules include, for example, patches, service packs, and where applicable, device drivers.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-5(3).1**

**Assessment Objective**

Determine if:
the organization defines critical software programs that the information system will prevent from being installed if such software programs are not signed with a recognized and approved certificate;

the information system prevents the installation of organization-defined critical software programs that are not signed with a certificate that is recognized and approved by the organization.

**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; security plan; change control records; information system audit records; other relevant documents or records.

**Test:** Information system mechanisms preventing installation of software programs not signed with an organization-approved certificate.

## CM-6 – Configuration Settings (High)

**Control**

The organization:
a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

**Implementation Standard(s)**

1. 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 all security configuration guidelines is as follows:
(a) CMS
(b) DHHS
(c) OMB
(d) NIST
(e) DISA.

**Guidance**

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AS-3, CM-2, CM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** CM-3, CM-8, SI-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-6.1**

**Assessment Objective**

Determine if:

the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed;

the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;

the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;

the organization implements the security configuration settings;

the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements;

the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with security configuration responsibilities.

**CM-6(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-6(1).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing the centralized management, application, and verification of configuration settings.

**CM-6(2) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to respond to unauthorized changes to network and system security-related configuration settings.

**Guidance**

Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring mandatory/organization-defined configuration settings, or in the extreme case, halting affected information system processing.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-6(2).1**

**Assessment Objective**

Determine if:
the organization defines configuration settings that, if modified by unauthorized changes, initiate the automated mechanisms to be employed to respond to such changes;

the organization employs automated mechanisms to respond to unauthorized changes to organization-defined configuration settings;

**Assessment Methods And Objects**

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

**Test:** Automated mechanisms implementing responses to unauthorized changes to configuration settings.

**CM-6(3) – Enhancement (High)**

**Control**

The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-6(3).1**

**Assessment Objective**

Determine if:
the organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability;

the organization ensures that such detected events are tracked, monitored, corrected, and available for historical purposes.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; procedures addressing incident response planning; information system design documentation; information system configuration settings and associated documentation; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities.

**CM-6(4) – Enhancement (High)**

**Control**

The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-6(4).1**

**Assessment Objective**

Determine if the information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.

**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; other relevant documents or records.

**Interview:** Organizational personnel with security configuration responsibilities.

| CM-7 – Least Functionality (High) | | |
|---|---|---|
| **Control**<br>The organization configures the information system to provide only essential capabilities and specifically disables, prohibits, or restricts the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled. | | |
| **Guidance**<br>Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential CMS operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, 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 server or web server, not both). The functions and services provided by CMS information systems, or individual components of CMS information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components 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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-3, CM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines for the information system prohibited or restricted:<br>- functions;<br>- ports;<br>- protocols;<br>- services; | | |

the organization configures the information system to provide only essential capabilities;

the organization configures the information system to specifically prohibit or restrict the use of organization-defined:
- functions;
- ports;
- protocols; and/or
- services;

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.

**Test:** Information system for disabling or restricting functions, ports, protocols, and services.

**CM-7(1) – Enhancement (High)**

**Control**

The organization reviews the information system within every three hundred sixty-five (365) days to identify and eliminate unnecessary functions, ports, protocols, and/or services.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-7(1).1**

**Assessment Objective**

Determine if:
the organization defines the frequency of information system reviews to identify and eliminate unnecessary:
- functions;
- ports;
- protocols; and/or
- services;

the organization reviews the information system in accordance with organization-defined frequency to identify and eliminate unnecessary:
- functions;
- ports;
- protocols; and/or
- services;

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the information system

**CM-7(2) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to prevent program execution in accordance with list of authorized or unauthorized software programs and rules authorizing the terms and conditions of software program usage.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-7(2).1**

**Assessment Objective**

Determine if:
the organization develops and maintains one or more of the following specifications to prevent software program execution on the information system:
- a list of software programs authorized to execute on the information system;
- a list of software programs not authorized to execute on the information system; and/or
- rules authorizing the terms and conditions of software program usage on the information system;

the organization employs automated mechanisms to prevent software program execution on the information system in accordance with the organization-defined specifications.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms preventing software program execution on the information system.

## CM-8 – Information System Component Inventory (High)

**Control**

The organization develops, documents, and maintains an inventory of information system components that:
a. Accurately reflects the current information system;
b. Is consistent with the authorization boundary of the information system;
c. Is at the level of granularity deemed necessary for tracking and reporting;
d. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and
e. Is available for review and audit by designated organizational officials.

**Guidance**

Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, 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.

| **Applicability:** All | **Reference(s):** FISCAM: CM-2, SM-1; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii) | **Related Controls Requirement(s):** CM-6 |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-8.1**

**Assessment Objective**

Determine if:
the organization defines information deemed necessary to achieve effective property accountability;

the organization develops, documents, and maintains an inventory of information system components that:
- accurately reflects the current information system;
- is consistent with the authorization boundary of the information system;
- is at the level of granularity deemed necessary for tracking and reporting;
- includes organization-defined information deemed necessary to achieve effective property accountability;
- is available for review and audit by designated organizational officials.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; other relevant documents or records.

**CM-8(1) – Enhancement (High)**

**Control**

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

| **Applicability:** All | **Reference(s):** HIPAA: 164.310(d)(1), 164.310(d)(2)(iii) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-8(1).1**

**Assessment Objective**

Determine if the organization updates the inventory of information system components as an integral part of component:
- installations;
- removals;
- information system updates;

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records.

**Interview:** Organizational personnel with information system installation and inventory responsibilities.

| CM-8(2) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. | | |
| **Guidance**<br>Organizations maintain the information system inventory to the extent feasible. Virtual machines, for example, can be difficult to monitor because they are not visible to the network when not in use. In such cases, the intent of this control enhancement is to maintain as up-to-date, complete, and accurate an inventory as is reasonable. | | |
| **Applicability:** All | **Reference(s):** HIPAA: 164.310(d)(1), 164.310(d)(2)(iii) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-8(2).1** | | |
| **Assessment Objective**<br>Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.<br>**Assessment Methods And Objects**<br>**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records.<br>**Test:** Automated mechanisms implementing information system component inventory management. | | |
| **CM-8(3) – Enhancement (High)** | | |
| **Control**<br>The organization:<br>(a) Employs automated mechanisms to scan the network no less than quarterly to detect the addition of unauthorized components/devices into the information system; and<br>(b) Disables network access by such components/devices or notifies designated organizational officials. | | |

**Guidance**

This control enhancement is applied in addition to the monitoring for unauthorized remote connections in AC-17 and for unauthorized mobile devices in AC-19. The monitoring for unauthorized components/devices on information system networks may be accomplished on an ongoing basis or by the periodic scanning of organizational networks for that purpose. Automated mechanisms can be implemented within the information system and/or in another separate information system or device.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-8(3).1**

**Assessment Objective**

Determine if:
the organization defines the frequency of employing automated mechanisms to detect the addition of unauthorized components/devices into the information system;

the organization employs automated mechanisms, in accordance with the organization-defined frequency, to detect the addition of unauthorized components/devices into the information system;

the organization disables network access by such components/devices or notifies designated organizational officials;

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system design documentation; information system inventory records; component installation records; change control records; other relevant documents or records.

**Test:** Automated mechanisms for detecting unauthorized components/devices on the information system.

**CM-8(4) – Enhancement (High)**

**Control**

The organization includes in property accountability information for information system components, a means for identifying by name and role individuals responsible for administering those components.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-8(4).1**

**Assessment Objective**

Determine if the organization includes in property accountability information for information system components, a means for identifying by name, position, or role, individuals responsible for administering those components.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records.

**CM-8(5) – Enhancement (High)**

**Control**

The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-8(5).1**

**Assessment Objective**

Determine if the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; component installation records; other relevant documents or records.

**Interview:** Organizational personnel with information system inventory responsibilities; organizational personnel with responsibilities for defining information system components within the authorization boundary of the system.

| CM-9 – Configuration Management Plan (High) | | |
|---|---|---|
| **Control**<br>The organization develops, documents, and implements a configuration management plan for the information system that:<br>a. Addresses roles, responsibilities, and configuration management processes and procedures;<br>b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and<br>c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items. | | |
| **Guidance**<br>Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: CM-9.1**

**Assessment Objective**

Determine if the organization develops, documents, and implements a configuration management plan for the information system that:
- addresses roles, responsibilities, and configuration management processes and procedures;
- defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management;
- establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing configuration management planning; security plan; other relevant documents or records.

# 6.0CONTINGENCY PLANNING (CP) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CP-1 – Contingency Planning Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-5, CP-1, CP-3, SM-1, SM-3; HIPAA: 164.308(a)(7)(i), 164.308(a)(7)(ii)(B); IRS-1075: 5.6.2.2#1.1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents contingency planning policy; | | |

the organization contingency planning policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities;

the organization develops and formally documents contingency planning procedures;

the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls;

the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities;

the organization reviews/updates the contingency planning policy and procedures within every three hundred sixty-five (365) days.

**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) |
| --- |
| **Control**<br>The organization:<br>a. Develops a Contingency Plan (CP) for the information system that:<br>- Identifies essential CMS missions and business functions and associated contingency requirements;<br>- Provides recovery objectives, restoration priorities, and metrics;<br>- Addresses contingency roles, responsibilities, assigned individuals with contact information;<br>- Addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure;<br>- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and<br>- Is reviewed and approved by designated officials within the organization;<br>b. Distributes copies of the CP plan to key contingency personnel (identified by name and/or by role) and organizational elements;<br>c. Coordinates contingency planning activities with incident handling activities;<br>d. Reviews the CP for the information system within every three hundred sixty-five (365) days;<br>e. Revises the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing; and<br>f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements. |
| **Guidance**<br>Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for CMS mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Copies of the current CP are stored in a secure location at an alternate site accessible by management and other key personnel. |

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-1, CP-2, CP-3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-2.1**

**Assessment Objective**

Determine if:
the organization develops a contingency plan for the information system that:
- identifies essential missions and business functions and associated contingency requirements;
- provides recovery objectives, restoration priorities, and metrics;
- addresses contingency roles, responsibilities, assigned individuals with contact information;
- addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;
-is reviewed and approved by designated officials within the organization;

the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan;

the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities.

**ASSESSMENT PROCEDURE: CP-2.2**

**Assessment Objective**

Determine if:
the organization coordinates contingency planning activities with incident handling activities;

the organization defines the frequency of contingency plan reviews;

the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;

the organization revises 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;

the organization communicates contingency plan changes to the key contingency personnel and organizational elements.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities.

**CP-2(1) – Enhancement (High)**

**Control**

The organization coordinates contingency plan development with organizational elements responsible for related plans.

**Guidance**

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Critical Infrastructure Plan, and Incident Response Plan.

| **Applicability:** All | **Reference(s):** HIPAA: 164.308(a)(7)(ii)(E); HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-2(1).1**

**Assessment Objective**

Determine if the organization coordinates the contingency plan development with other organizational elements responsible for related plans.

**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) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. | | |
| **Applicability:** All | **Reference(s):** HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-2(2).1** | | |
| **Assessment Objective**<br>Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records.<br>**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities. | | |
| **CP-2(3) – Enhancement (High)** | | |
| **Control**<br>The organization plans for the resumption of systems included on the CMS Critical Infrastructure Protection (CIP) list within twelve (12) hours and for the resumption of other essential missions and business functions within one (1) week of contingency plan activation. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-2(3).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization plans for the resumption of systems included on the CMS CIP list within twelve (12) hours of contingency plan activation.<br>the organization plans for the resumption of other essential missions and business functions within one (1) week of contingency plan activation. | | |

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; business impact assessment; other related plans; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities.

**CP-3 – Contingency Training (High)**

**Control**

The organization trains operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days.

**Guidance**

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 confirmed that appropriate training has been completed.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2; HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-3.1**

**Assessment Objective**

Determine if:

the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is at least annually;

the organization provides refresher training in accordance with organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning, plan implementation, and training responsibilities.

| CP-3(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations. | | |
| **Applicability:** All | **Reference(s):** HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-3(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization incorporates simulated events into contingency training;<br>the incorporation of simulated events into contingency training facilitates effective response by personnel in crisis situations.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.<br>**Interview:** Organizational personnel with contingency planning, plan implementation, and training responsibilities. | | |
| **CP-4 – Contingency Plan Testing and Exercises (High)** | | |
| **Control**<br>The organization:<br>a. Tests and/or exercises the contingency plan for the CMS information system within every three hundred sixty-five (365) days using defined tests and exercises, such as the tabletop test in accordance with the current CMS contingency plan procedure to determine the plan's effectiveness and the organization's readiness to execute the plan; and<br>b. Documents and reviews the contingency plan test/exercise results and initiates reasonable and appropriate corrective actions to close or reduce the impact of contingency plan failures and deficiencies. | | |

**Guidance**

There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on CMS operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-2, CP-4; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-4.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted;

the organization defines in the security plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is at least annually;

the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;

the organization reviews the contingency plan test/exercise results and takes corrective actions.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises.

**CP-4(1) – Enhancement (High)**

**Control**

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

**Guidance**

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Critical Infrastructure Plan, and Incident Response Plan.

| **Applicability:** All | **Reference(s):** HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-4(1).1**

**Assessment Objective**

Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.

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

**CP-4(2) – Enhancement (High)**

**Control**

The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

| **Applicability:** All | **Reference(s):** HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-4(2).1**

**Assessment Objective**

Determine if the organization conducts contingency plan testing/exercises at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

**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; other relevant documents or records.

**CP-4(4) – Enhancement (High)**

**Control**

The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-4(4).1**

**Assessment Objective**

Determine if the organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system recovery and reconstitution responsibilities; organizational personnel with contingency plan testing and/or exercise responsibilities.

**CP-5 – Contingency Plan Update (High)**

**Control**

[Withdrawn: Incorporated into CP-2].

**CP-6 – Alternate Storage Site (High)**

**Control**

The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.

**Guidance**

The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with CMS' recovery time objectives and recovery point objectives.

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-2, CP-3; IRS-1075: 5.6.2.2#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-6.1**

**Assessment Objective**

Determine if:
the organization establishes an alternate storage site;

the organization initiates necessary alternate storage site agreements to permit the storage and recovery of information system backup information.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records.

**CP-6(1) – Enhancement (High)**

**Control**

The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.

**Guidance**

Hazards of concern to the organization are typically defined in an organizational assessment of risk.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-6(1).1**

**Assessment Objective**

Determine if:
the contingency plan identifies the primary storage site hazards;

the alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

**CP-6(2) – Enhancement (High)**

**Control**

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-6(2).1**

**Assessment Objective**

Determine if the alternate storage site is configured to facilitate recovery operations in accordance with recovery time objectives and recovery point objectives.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate storage site; other relevant documents or records.

**CP-6(3) – Enhancement (High)**

**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.

**Guidance**

Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-6(3).1**

**Assessment Objective**

Determine if:
the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster;

the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.

**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; other relevant documents or records.

**CP-7 – Alternate Processing Site (High)**

**Control**

The organization:
a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; and
b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the time period for resumption specified in Implementation Standard 1.

**Implementation Standard(s)**

1. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of systems included on the CMS Critical Infrastructure Protection (CIP) list within twelve (12) hours and resumption of other essential missions and business functions within one (1) week of contingency plan activation.

**Guidance**

Equipment and supplies required to resume operations within the CMS-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with CMS recovery time objectives.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, CP-3; IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-7.1**

**Assessment Objective**

Determine if:
the organization establishes an alternate processing site;

the organization includes necessary alternate processing site agreements to permit the resumption of information system operations within the time period specified in Implementation Standard 1;

the equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the time period for resumption specified in Implementation Standard 1;

the organization meets all the requirements specified in the applicable implementation standard(s);

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; security plan; spare equipment and supplies at alternate processing site; equipment and supply contracts; service level agreements; other relevant documents or records.

**CP-7(1) – Enhancement (High)**

**Control**

The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.

**Guidance**

Hazards that might affect the information system are typically defined in the risk assessment.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-7(1).1**

**Assessment Objective**

Determine if:
the contingency plan identifies the primary processing site hazards;

the alternate processing site is separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

**CP-7(2) – Enhancement (High)**

**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.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-7(2).1**

**Assessment Objective**

Determine if:
the organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster;

the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

**CP-7(3) – Enhancement (High)**

**Control**

the organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

| ASSESSMENT PROCEDURE: CP-7(3).1 | | |
|---|---|---|
| **Assessment Objective**<br>Determine if alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records. | | |
| **CP-7(4) – Enhancement (High)** | | |
| **Control**<br>The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential CMS missions and business functions. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-7(4).1** | | |
| **Assessment Objective**<br>Determine if the alternate processing site is configured so that it is ready to be used as the operational site to support essential missions and business functions.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records.<br>**Test:** Information system at the alternate processing site. | | |
| **CP-7(5) – Enhancement (High)** | | |
| **Control**<br>The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: CP-7(5).1**

**Assessment Objective**

Determine if the alternate processing site provides information security measures equivalent to that of the primary site.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

**CP-8 – Telecommunications Services (High)**

**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 period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable.

**Implementation Standard(s)**

1. Ensure alternate telecommunications service agreements are in place to permit resumption of systems included on the CMS Critical Infrastructure Protection (CIP) list within twelve (12) hours and resumption of other essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, CP-3; IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-8.1**

**Assessment Objective**

Determine if:

the organization establishes alternate telecommunications services to support the information system;

the organization establishes necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for CMS missions and business functions within the time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; list of essential missions and business functions; other relevant documents or records.

**CP-8(1) – Enhancement (High)**

**Control**

The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-8(1).1**

**Assessment Objective**

Determine if:
the organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements;

the organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

**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; other relevant documents or records.

**CP-8(2) – Enhancement (High)**

**Control**

The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-8(2).1**

**Assessment Objective**

Determine if the organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

**CP-8(3) – Enhancement (High)**

**Control**

The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-8(3).1**

**Assessment Objective**

Determine if:
the organization identifies the primary provider's telecommunications service hazards;

the alternate telecommunications service providers are separated from the primary telecommunications service providers so as not to be susceptible to the same hazards.

**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; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

| CP-8(4) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization requires primary and alternate telecommunications service providers to have contingency plans. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-8(4).1** | | |
| **Assessment Objective**<br>Determine if the organization requires primary and alternate telecommunications service providers to have contingency plans.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.<br>**Interview:** Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers. | | |
| **CP-9 – Information System Backup (High)** | | |
| **Control**<br>The organization:<br>a. Conducts backups of user-level information contained in the CMS information system in accordance with the frequency specified in Implementation Standard 1;<br>b. Conducts backups of system-level information contained in the CMS information system in accordance with the frequency specified in Implementation Standard 1;<br>c. Conducts backups of CMS information system documentation including security-related documentation and other forms of data, including paper records; and<br>d. Protects the confidentiality and integrity of CMS backup information at the storage location.<br>**Implementation Standard(s)**<br>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.<br>2. (For PII only) Ensure that a current, retrievable, copy of PII is available before movement of servers. | | |

**Guidance**

System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control.

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.

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-2; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6 | **Related Controls**<br>**Requirement(s):** MP-4, MP-5 |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-9.1**

**Assessment Objective**

Determine if:

the organization backs up user-level information in accordance with the frequency specified in Implementation Standard 1;

the organization backs up system-level information in accordance with the frequency specified in Implementation Standard 1;

the organization backs up information system documentation (including security-related information and other forms of data).

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; backup storage location(s); information system backup logs or records; other relevant documents or records.

**Interview:** Organizational personnel with information system backup responsibilities.

**ASSESSMENT PROCEDURE: CP-9.2**

**Assessment Objective**

Determine if the organization protects the confidentiality and integrity of backup information at the storage location.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; information system configuration settings and associated documentation; backup storage location(s); other relevant documents or records.

**Interview:** Organizational personnel with information system backup responsibilities.

**CP-9(1) – Enhancement (High)**

**Control**

The organization tests backup information following each backup to verify media reliability and information integrity.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-9(1).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the frequency of information system backup testing;

the organization conducts information system backup testing in accordance with organization-defined frequency to verify backup media reliability and information integrity.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; information system backup test results; backup storage location(s); other relevant documents or records.

**CP-9(2) – Enhancement (High)**

**Control**

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-9(2).1**

**Assessment Objective**

Determine if the organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

**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; other relevant documents or records.

**CP-9(3) – Enhancement (High)**

**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.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-9(3).1**

**Assessment Objective**

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); other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information system backup responsibilities.

**CP-9(4) – Enhancement (High)**

**Control**

[Withdrawn: Incorporated into CP-9].

| CP-10 – Information System Recovery and Reconstitution (High) | | |
|---|---|---|
| **Control**<br>The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.<br>**Implementation Standard(s)**<br>1. Secure information system recovery and reconstitution includes, but not limited to:<br>(a) Reset all system parameters (either default or organization-established),<br>(b) Reinstall patches,<br>(c) Reestablish configuration settings,<br>(d) Reinstall application and system software, and<br>(e) Fully test the system. | | |
| **Guidance**<br>Recovery is executing information system contingency plan activities to restore essential CMS missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on CMS priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. | | |
| **Applicability:** All | **Reference(s):** FISCAM: CP-2, CP-3, CP-4; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-10.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure; | | |

the organization provides for the recovery of the information system after a failure or other contingency in a trusted, secure, and verifiable manner.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Test:** Automated mechanisms and/or manual procedures for implementing information system recovery and reconstitution operations.

**CP-10(1) – Enhancement (High)**

**Control**

[Withdrawn: Incorporated into CP-4].

**CP-10(2) – Enhancement (High)**

**Control**

The information system implements transaction recovery for systems that are transaction-based.

**Guidance**

Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-10(2).1**

**Assessment Objective**

Determine if the information system implements transaction recovery for systems that are transaction-based.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing transaction recovery capability.

| CP-10(3) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization provides compensating security controls for circumstances that inhibit recovery and reconstitution to a known state. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-10(3).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state;<br>the organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan test procedures; security plan; other relevant documents or records.<br>**Interview:** Organizational personnel with information system recovery and reconstitution responsibilities. | | |
| **CP-10(4) – Enhancement (High)** | | |
| **Control**<br>The organization provides the capability to reimage information system components and support target recovery times from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: CP-10(4).1**

**Assessment Objective**

Determine if:
the organization defines the time-periods within which information system components must be reimaged from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components;

the organization provides the capability to reimage information system components, within organization-defined time-periods, from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system recovery and reconstitution responsibilities.

# 7.0IDENTIFICATION AND AUTHENTICATION (IA) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **IA-1 – Identification and Authentication Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.3.1#1.1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents identification and authentication policy; | | |

the organization identification and authentication policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities;

the organization develops and formally documents identification and authentication procedures;

the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls;

the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities;

the organization reviews/updates the identification and authentication policy and procedures within every three hundred sixty-five (365) days.

**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)**

**Control**

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

**Implementation Standard(s)**

1. Require the use of system and/or network authenticators and unique user identifiers.
2. Help desk support requires user identification for any transaction that has information security implications.

**Guidance**

Organizational users (i.e., CMS information system users) include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to CMS information systems is defined as either local or network. Local access is any access to a CMS information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to a CMS information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.

The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 5.6.3.1#1.2, 5.6.3.3#2.3 | **Related Controls Requirement(s):** AC-14, AC-17, MA-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2.1**

**Assessment Objective**

Determine if:

the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Test:** Automated mechanisms implementing identification and authentication capability for the information system.

**IA-2(1) – Enhancement (High)**

**Control**

The information system uses multifactor authentication for network access to privileged accounts.

| **Applicability:** All | **Reference(s):** HIPAA: 164.312(d); IRS-1075: 5.6.3.1#1.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(1).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for network access to privileged accounts.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing identification and authentication capability for the information system.

**IA-2(2) – Enhancement (High)**

**Control**

The information system uses multifactor authentication for network access to non-privileged accounts.

| **Applicability:** All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, Part A, Part B, QIC, RAC, SS, ZPIC | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(2).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for network access to non-privileged accounts.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing identification and authentication capability for the information system.

**IA-2(3) – Enhancement (High)**

**Control**

The information system uses multifactor authentication for local access to privileged accounts.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(3).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for local access to privileged accounts.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing identification and authentication capability for the information system.

## IA-2(4) – Enhancement (High)

**Control**

The information system uses multifactor authentication for local access to non-privileged accounts.

| **Applicability:** All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, Part A, Part B, QIC, RAC, SS, ZPIC | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(4).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for local access to non-privileged accounts.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing identification and authentication capability for the information system.

## IA-2(8) – Enhancement (High)

**Control**

The information system uses replay resistant authentication mechanisms for network access to privileged accounts.

| | | |
|---|---|---|
| **Guidance**<br>An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-2(8).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts;<br>the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Test:** Automated mechanisms implementing identification and authentication capability for the information system. | | |
| **IA-2(9) – Enhancement (High)** | | |
| **Control**<br>The information system uses replay resistant authentication mechanisms for network access to non-privileged accounts. | | |
| **Guidance**<br>An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

| **ASSESSMENT PROCEDURE: IA-2(9).1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization defines the replay-resistant authentication mechanisms to be used for network access to non-privileged accounts;<br>the information system uses the organization-defined replay-resistant authentication mechanisms for network access to non-privileged accounts.<br>**Assessment Methods And Objects**<br>**Examine:** Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.<br>**Test:** Automated mechanisms implementing identification and authentication capability for the information system. | | |
| **IA-3 – Device Identification and Authentication (High)** | | |
| **Control**<br>The information system uniquely identifies and authenticates specific and/or types of devices before establishing a connection. | | |
| **Guidance**<br>The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AC-2; IRS-1075: 5.6.3.1#1.2 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: IA-3.1**

**Assessment Objective**

Determine if:
the organization defines the specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system;

the information system uniquely identifies and authenticates the organization-defined devices before establishing a connection to the information system.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing device identification and authentication.

**IA-4 – Identifier Management (High)**

**Control**

The organization manages CMS information system identifiers for users and devices by:
a. Receiving authorization from a designated organizational official to assign a user or device identifier;
b. Selecting an identifier that uniquely identifies an individual or device;
c. Assigning the user identifier to the intended party or the device identifier to the intended device;
d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired; and
e. Disabling the user identifier after the time period of inactivity specified in Implementation Standard 1 and deleting disabled accounts during the annual re-certification process.

**Implementation Standard(s)**

1. Disable user identifiers after ninety (90) days of inactivity.

**Guidance**

Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system).

Reviews and validation of system users' accounts are conducted to ensure the continued need for access to a system. Identifier management is applicable to shared information system accounts (i.e., guest and anonymous).

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AC-4, AS-2; IRS-1075: 5.6.3.1#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-4.1**

**Assessment Objective**

Determine if:

the organization manages information system identifiers for users and devices by:

- receiving authorization from a designated organizational official to assign a user or device identifier;
- selecting an identifier that uniquely identifies an individual or device;
- assigning the user identifier to the intended party or the device identifier to the intended device;
- preventing reuse of user or device identifiers for the organization-defined time period;
- disabling the user identifier after the organization-defined time period of inactivity;

the organization defines in the security plan, explicitly or by reference, the time period of inactivity after which a user identifier is to be disabled.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records.

**Interview:** Organizational personnel with identifier management responsibilities.

| IA-5 – Authenticator Management (High) |
|---|
| **Control**<br>The organization manages CMS information system authenticators for users and devices by:<br>a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;<br>b. Establishing initial authenticator content for authenticators defined by the organization;<br>c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;<br>d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;<br>e. Changing default content of authenticators upon information system installation;<br>f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);<br>g. Changing/refreshing password authenticators as defined in IA-5(1);<br>h. Protecting authenticator content from unauthorized disclosure and modification; and<br>i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. |
| **Guidance**<br>User 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). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The CMS information system supports user authenticator management by security 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 verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost 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. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2; IRS-1075: 5.6.3.1#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-5.1**

**Assessment Objective**

Determine if:
the organization defines the time period (by authenticator type) for changing/refreshing authenticators;

the organization manages information system authenticators for users and devices by:
- verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- establishing initial authenticator content for authenticators defined by the organization;
- ensuring that authenticators have sufficient strength of mechanism for their intended use;
- establishing and implementing administrative procedures for initial authenticator distribution;
- establishing and implementing administrative procedures for lost/compromised or damaged authenticators;
- establishing and implementing administrative procedures for revoking authenticators;
- changing default content of authenticators upon information system installation;
- establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);
- changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;
- protecting authenticator content from unauthorized disclosure and modification;
- requiring users to take, and having devices implement, specific measures to safeguard authenticators.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; 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) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The CMS information system, for password-based authentication:<br>(a) Automatically forces users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days;<br>(b) Prohibits the use of dictionary names or words;<br>(c) Enforces minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lower-case letters, and numbers) and special characters;<br>(d) Enforces at least a minimum of four (4) changed characters when new passwords are created;<br>(e) Encrypts passwords in storage and in transmission;<br>(f) Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum; and<br>(g) Prohibits password reuse for six (6) generations prior to reuse. | | |
| **Guidance**<br>This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does not apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-5(1).1** | | |
| **Assessment Objective**<br>Determine if the information system, for password-based authentication:<br>- enforces the minimum password complexity standards that meet the organization-defined requirements;<br>- enforces the organization-defined minimum number of characters that must be changed when new passwords are created;<br>- encrypts passwords in storage and in transmission;<br>- enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters;<br>- prohibits password reuse for the organization-defined number of generations. | | |

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing authenticator management functions.

**IA-5(2) – Enhancement (High)**

**Control**

The CMS information system, for PKI-based authentication:
(a) Validates certificates by constructing a certification path with status information to an accepted trust anchor;
(b) Enforces authorized access to the corresponding private key; and
(c) Maps the authenticated identity to the user account.

**Guidance**

Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-5(2).1**

**Assessment Objective**

Determine if the information system, for PKI-based authentication:
- validates certificates by constructing a certification path with status information to an accepted trust anchor;
- enforces authorized access to the corresponding private key;
- maps the authenticated identity to the user account.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for PKI-based authentication management.

**Test:** Automated mechanisms implementing PKI-based authenticator management functions.

| IA-5(3) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization requires that the registration process to receive hardware tokens be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-5(3).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official;<br>the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).<br>**Assessment Methods And Objects**<br>**Examine:** Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; other relevant documents or records.<br>**Interview:** Organizational personnel with authenticator management responsibilities. | | |
| **IA-6 – Authenticator Feedback (High)** | | |
| **Control**<br>The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. | | |
| **Guidance**<br>The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2; IRS-1075: 5.6.3.1#1.2 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: IA-6.1**

**Assessment Objective**

Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing authenticator feedback.

**IA-7 – Cryptographic Module Authentication (High)**

**Control**

The information system uses 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-7.1**

**Assessment Objective**

Determine if the information system uses 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.

**Assessment Methods And Objects**

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

**Test:** Automated mechanisms implementing cryptographic module authentication.

| IA-8 – Identification and Authentication (Non-Organizational Users) (High) | | |
|---|---|---|
| **Control**<br>The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). | | |
| **Guidance**<br>Non-organizational users include all CMS information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with 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). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered 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 to CMS operations, CMS assets, individuals, other organizations, and the Nation. Identification and authentication requirements for CMS information system access by organizational users are described in IA-2. If E-Authentication is used, refer to ARS Appendix D: E-authentication Standard. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-8.1** | | |
| **Assessment Objective**<br>Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).<br>**Assessment Methods And Objects**<br>**Examine:** Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records.<br>**Test:** Automated mechanisms implementing identification and authentication capability for the information system. | | |

# 8.0INCIDENT RESPONSE (IR) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **IR-1 – Incident Response Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-1, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents incident response policy; | | |

the organization incident response policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities;

the organization develops and formally documents incident response procedures;

the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls;

the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities;

the organization reviews/updates the incident response policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Incident response policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with incident response responsibilities.

**IR-2 – Incident Response Training (High)**

**Control**

The organization:
a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and
b. Provides refresher training within every three hundred sixty-five (365) days.

**Guidance**

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Incident response training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. 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 basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
(4) CIOs, IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.2.6#2.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-2.1**

**Assessment Objective**

Determine if:
the organization identifies personnel with incident response roles and responsibilities with respect to the information system;

the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;

incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually;

the organization provides refresher incident response training in accordance with organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records.

**Interview:** Organizational personnel with incident response training and operational responsibilities.

**IR-2(1) – Enhancement (High)**

**Control**

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-2(1).1**

**Assessment Objective**

Determine if the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response training; incident response training material; other relevant documents or records.

**Interview:** Organizational personnel with incident response training and operational responsibilities.

**IR-2(2) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to provide a more thorough and realistic training environment.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-2(2).1**

**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; automated mechanisms supporting incident response training; other relevant documents or records.

**Interview:** Organizational personnel with incident response training and operational responsibilities.

**IR-3 – Incident Response Testing and Exercises (High)**

**Control**

The organization tests and/or exercises the incident response capability for the information system within every three hundred sixty-five (365) days using reviews, analyses, and simulations to determine the incident response effectiveness and documents the results.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.2.6#2.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-3.1**

**Assessment Objective**

Determine if:
the organization defines incident response tests/exercises;

the organization defines in the security plan, explicitly or by reference, the frequency of incident response tests/exercises and the frequency is at least annually;

the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;

the organization documents the results of incident response tests/exercises;

the organization determines the effectiveness of the incident response capability.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing material; incident response test results; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with incident response testing responsibilities.

**IR-3(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

**Guidance**

Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the incident response capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-3(1).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability for the information system.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing documentation; automated mechanisms supporting incident response tests/exercises; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with incident response testing responsibilities.

**IR-4 – Incident Handling (High)**

**Control**

The organization:
a. Implements an incident handling capability using CMS Information Security Incident Handling and Breach Notification Procedures;
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 Standard(s)**

1. Document relevant information related to a security incident according to CMS Information Security Incident Handling and Breach Notification Procedures.
2. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.
3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure, including isolation or system disconnect.

**Guidance**

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3 | **Related Controls Requirement(s):** AU-6, PE-6, SI-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-4.1**

**Assessment Objective**

Determine if:
the organization implements an incident handling capability for security incidents that includes:
- preparation;
- detection and analysis;
- containment;
- eradication;
- recovery;

the organization coordinates incident handling activities with contingency planning activities;

the organization incorporates lessons learned from ongoing incident handling activities into:
- incident response procedures;
- training;
- testing/exercises;

the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.

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; other relevant documents or records.

**Interview:** Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities.

**Test:** Incident handling capability for the organization.

**IR-4(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to support the incident handling process.

**Guidance**

An online incident management system is an example of an automated mechanism.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-4(1).1**

**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; other relevant documents or records.

**Interview:** Organizational personnel with incident handling responsibilities.

**IR-5 – Incident Monitoring (High)**

**Control**

The organization tracks and documents information system security incidents.

**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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, SM-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#2.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-5.1**

**Assessment Objective**

Determine if the organization tracks and documents information system security incidents.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with incident monitoring responsibilities.

**Test:** Incident monitoring capability for the organization.

| IR-5(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. | | |
| **Guidance**<br>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 (CIRCs) or other electronic databases of incidents. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-5(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization employs automated mechanisms to assist in the tracking of security incidents;<br>the organization employs automated mechanisms to assist in the collection of security incident information;<br>the organization employs automated mechanisms to assist in the analysis of security incident information. | | |
| **Assessment Methods And Objects**<br>**Examine:** Incident response policy; procedures addressing incident monitoring; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting incident monitoring; incident response plan; other relevant documents or records.<br>**Interview:** Organizational personnel with incident monitoring responsibilities.<br>**Test:** Automated mechanisms assisting in tracking of security incidents and in the collection and analysis of incident information. | | |

| IR-6 – Incident Reporting (High) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Requires personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current CMS Information Security Incident Handling and Breach Analysis/Notification Procedure; and<br>b. Reports security incident information to designated authorities. | | |
| **Guidance**<br>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. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. CMS requires that events and confirmed security incidents must be reported to the CMS IT Service Desk in accordance with established procedures. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-6.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current CMS Information Security Incident Handling and Breach Analysis/Notification Procedure;<br>the organization reports security incident information to designated authorities.<br>**Assessment Methods And Objects**<br>**Examine:** Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records.<br>**Interview:** Organizational personnel with incident reporting responsibilities. | | |

| IR-6(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms to assist in the reporting of security incidents. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-6(1).1** | | |
| **Assessment Objective**<br>Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.<br>**Assessment Methods And Objects**<br>**Examine:** Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; incident response plan; other relevant documents or records.<br>**Interview:** Organizational personnel with incident reporting responsibilities. | | |
| **IR-7 – Incident Response Assistance (High)** | | |
| **Control**<br>The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents. | | |
| **Guidance**<br>Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. The CMS IT Service Desk is available to offer advice to users of a CMS information system. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>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; | | |

the incident response support resource is an integral part of the organization's incident response capability.

**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.

**IR-7(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

**Guidance**

Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-7(1).1**

**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 assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with incident response support and assistance responsibilities; organizational personnel that require incident response support and assistance.

| IR-8 – Incident Response Plan (High) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Develops an incident response plan that:<br>- Provides the organization with a roadmap for implementing its incident response capability;<br>- Describes the structure and organization of the incident response capability;<br>- Provides a high-level approach for how the incident response capability fits into the overall organization;<br>- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;<br>- Defines reportable incidents;<br>- Provides metrics for measuring the incident response capability within the organization.<br>- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and<br>- Is reviewed and approved by designated officials within the organization;<br>b. Distributes copies of the incident response plan to incident response personnel and organizational elements;<br>c. Reviews the incident response plan within every three hundred sixty-five (365) days;<br>d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and<br>e. Communicates incident response plan changes to incident response personnel and organizational elements. | | |
| **Guidance**<br>It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: IR-8.1**

**Assessment Objective**

Determine if the organization develops an incident response plan that:
- provides the organization with a roadmap for implementing its incident response capability;
- describes the structure and organization of the incident response capability;
- provides a high-level approach for how the incident response capability fits into the overall organization;
- meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- defines reportable incidents;
- provides metrics for measuring the incident response capability within the organization;
- defines the resources and management support needed to effectively maintain and mature an incident response capability;
- is reviewed and approved by designated officials within the organization.

**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 planning responsibilities.

**ASSESSMENT PROCEDURE: IR-8.2**

**Assessment Objective**

Determine if:
the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;

the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan;

the organization reviews the incident response plan in accordance with the organization-defined frequency;

the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.

**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 planning responsibilities.

# 9.0MAINTENANCE (MA) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **MA-1 – System Maintenance Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, CM-5, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system maintenance policy; | | |

the organization system maintenance policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities;

the organization develops and formally documents system maintenance procedures;

the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls;

the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities;

the organization reviews/updates the information system maintenance policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

| MA-2 – Controlled Maintenance (High) | | |
|---|---|---|
| **Control**<br>The organization:<br>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;<br>b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;<br>c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;<br>d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and<br>e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.<br>**Implementation Standard(s)**<br>1. (For PII only) In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | | |
| **Guidance**<br>The control is intended to address the information security aspects of the organization's CMS information system maintenance program. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. | | |
| **Applicability:** All; Optional for SS | **Reference(s):** FISCAM: AC-6, CP-2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MA-2.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization 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; | | |

the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** Facility documentation (such as floor plan and elevation drawings) are updated when repairs and modifications cause changes to the physical components of the facility containing PII.

**Interview:** Organizational personnel with information system maintenance responsibilities.

**Interview:** Organizational personnel, with facility management responsibilities.

**MA-2(1) – Enhancement (High)**

**Control**

the organization maintains maintenance records for the information system that include:
- date and time of maintenance;
- name of the individual performing the maintenance;
- name of escort, if necessary;
- a description of the maintenance performed;
- a list of equipment removed or replaced (including identification numbers, if applicable).

| **Applicability:** All; Optional for SS | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-2(1).1**

**Assessment Objective**

Determine if the organization maintains maintenance records for the information system that include:
- date and time of maintenance;
- name of the individual performing the maintenance;
- name of escort, if necessary;
- description of the maintenance performed; and
- list of equipment removed or replaced (including identification numbers, if applicable).

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records.

**MA-2(2) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

| **Applicability:** All; Optional for SS | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-2(2).1**

**Assessment Objective**

Determine if:
the organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required;

the organization employs automated mechanisms to product up-to-date, accurate, complete, and available records of all maintenance and repair actions needed, in process and complete.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing controlled maintenance for the information system; automated mechanisms supporting information system maintenance activities; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

| MA-3 – Maintenance Tools (High) | | |
|---|---|---|
| **Control**<br>The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools. | | |
| **Guidance**<br>The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping", "ls", "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, CP-2; IRS-1075: 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MA-3.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization approves, controls, and monitors the use of information system maintenance tools;<br>the organization maintains information system maintenance tools on an ongoing basis.<br>**Assessment Methods And Objects**<br>**Examine:** Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records. | | |
| **MA-3(1) – Enhancement (High)** | | |
| **Control**<br>The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. | | |
| **Guidance**<br>Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system. | | |

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-3(1).1**

**Assessment Objective**

Determine if the organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

**MA-3(2) – Enhancement (High)**

**Control**

The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-3(2).1**

**Assessment Objective**

Determine if the organization checks all media containing diagnostic and test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

**Test:** Media checking process for malicious code detection.

| MA-3(3) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>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, in writing, from the CMS CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MA-3(3).1** | | |
| **Assessment Objective**<br>Determine if the organization prevents the unauthorized removal of maintenance equipment by one of the following:<br>- verifying that there is no organizational information contained on the equipment;<br>- sanitizing or destroying the equipment;<br>- retaining the equipment within the facility; or<br>- obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.<br>**Assessment Methods And Objects**<br>**Examine:** Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records.<br>**Interview:** Organizational personnel with information system maintenance responsibilities. | | |

| MA-4 – Non-Local Maintenance (High) | | |
|---|---|---|
| **Control**<br>The organization prohibits non-local CMS system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:<br>a. Monitors and controls non-local maintenance and diagnostic activities;<br>b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;<br>c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;<br>d. Maintains records for non-local maintenance and diagnostic activities; and<br>e. Terminates all sessions and network connections when non-local maintenance is completed.<br>**Implementation Standard(s)**<br>1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service. | | |
| **Guidance**<br>Non-local 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. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. 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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, SM-7; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** IA-2, MP-6 |
| **ASSESSMENT PROCEDURE: MA-4.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization prohibits non-local CMS system maintenance unless explicitly authorized, in writing, by the CIO; | | |

if authorized, the organization monitors and controls non-local maintenance and diagnostic activities;

if authorized, the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools;

if authorized, the organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;

if authorized, the organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;

if authorized, the organization terminates all sessions and network connections when non-local maintenance is completed.

if authorized, the organization maintains records for non-local maintenance and diagnostic activities;

if authorized, the organization (or information system in certain cases) terminates all sessions and network connections when non-local maintenance or diagnostics is completed.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

**MA-4(1) – Enhancement (High)**

**Control**

The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-4(1).1**

**Assessment Objective**

Determine if:
the organization audits non-local maintenance and diagnostic sessions;

designated organizational personnel review the maintenance records of the sessions.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; maintenance records; audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

**MA-4(2) – Enhancement (High)**

**Control**

The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-4(2).1**

**Assessment Objective**

Determine if the organization documents the installation and use of non-local maintenance and diagnostic connections in the security plan for the information system.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; maintenance records; audit records; other relevant documents or records.

**MA-4(3) – Enhancement (High)**

**Control**

The organization:
(a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or
(b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to sensitive information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-4(3).1**

**Assessment Objective**

Determine if:
the organization requires and ensures non-local maintenance and diagnostic services from an information system that implements a level of security at least as high as the level of security implemented on the information system being serviced; or

the organization removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities;

the organization after the removed component service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting to the information system.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; service provider contracts and/or service level agreements; maintenance records; audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities; information system maintenance provider.

**MA-5 – Maintenance Personnel (High)**

**Control**

The organization:
a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and
b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

**Guidance**

Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, SM-7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-5.1**

**Assessment Objective**

Determine if:
the organization establishes a process for maintenance personnel authorization;

the organization maintains a current list of authorized maintenance organizations or personnel;

personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with information system maintenance responsibilities.

**MA-6 – Timely Maintenance (High)**

**Control**

The organization obtains maintenance support and/or spare parts for CMS critical systems and applications (including Major Applications [MA] and General Support Systems [GSS] and their components) within twenty-four (24) hours of failure.

**Guidance**

The organization specifies those CMS information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-6.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, CMS critical information system and applications (including MA and GSS and their components) for which it will obtain maintenance support and/or spare parts;

the organization obtains maintenance support and/or spare parts for CMS critical information systems and applications (including MA and GSS and their components) within twenty-four (24) hours of failure.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with information system maintenance responsibilities.

# *10.0* MEDIA PROTECTION (MP) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **MP-1 – Media Protection Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.<br>**Implementation Standard(s)**<br>1. (For PII only) Semi-annual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SM-1, SM-3; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents media protection policy; | | |

the organization media protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities;

the organization develops and formally documents media protection procedures;

the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls;

the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities.

the organization reviews/updates the media protection policy and procedures within every three hundred sixty-five (365) days.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Media protection policy and procedures; other relevant documents or records.

**Examine:** PII semiannual inventory reports; other relevant documents or records.

**Interview:** Organizational personnel with information system media protection responsibilities.

**MP-2 – Media Access (High)**

**Control**

The organization restricts access to CMS sensitive digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.

**Guidance**

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AC-6, BP-3; HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-2.1**

**Assessment Objective**

Determine if:
the organization defines:
- digital and non-digital media requiring restricted access;
- individuals authorized to access the media;
- security measures taken to restrict access;

the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system media protection responsibilities.

| MP-2(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. | | |
| **Guidance**<br>This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices). | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-2(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization employs automated mechanisms to restrict access to media storage areas;<br>the organization employs automated mechanisms to audit access attempts and access granted to media storage areas. | | |
| **Assessment Methods And Objects**<br>**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 devices; access control records; audit records; other relevant documents or records.<br>**Test:** Automated mechanisms implementing access restrictions to media storage areas. | | |
| **MP-3 – Media Marking (High)** | | |
| **Control**<br>The organization:<br>a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and<br>b. Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment. | | |

**Guidance**

The term marking is used when referring to the application or use of human-readable security attributes. The term labeling is used when referring to the application or use of security attributes with regard to internal data structures within the information system (see AC-16, Security Attributes). Removable information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Organizations may extend the scope of this control to include information system output devices containing sensitive information, including, for example, monitors and printers. Marking of removable media and information system output is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; IRS-1075: 4.6#1, 5.1#1.2, 5.3#2.1-2, 5.3#3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-3.1**

**Assessment Objective**

Determine if:
the organization defines removable media types and information system output that require marking;

the organization marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information;

the organization defines:
- removable media types and information system output exempt from marking;
- controlled areas designated for retaining removable media and information output exempt from marking;

removable media and information system output exempt from marking remain within designated controlled areas.

**Assessment Methods And Objects**

**Examine:** Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and information system output; other relevant documents or records.

**Interview:** Organizational personnel with information system media protection and marking responsibilities.

| MP-4 – Media Storage (High) |
|---|
| **Control**<br>The organization:<br>a. Physically controls and securely stores digital and non-digital media within controlled areas using safeguards prescribed for the highest system security level of the information ever recorded on it;<br>b. Protects CMS information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.<br>**Implementation Standard(s)**<br>1. (For PII only) Evaluate employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance.<br>2. (For PII only) If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information. |
| **Guidance**<br>Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting CMS information and/or CMS information system.<br>An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on CMS or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection.<br>As part of a defense-in-depth strategy, the organization considers routinely encrypting CMS information at rest on selected secondary storage devices. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AC-6; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1 | **Related Controls Requirement(s):** AC-19, CP-9, CP-9(4), RA-2, SC-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-4.1**

**Assessment Objective**

Determine if:
the organization defines:
- types of digital and non-digital media physically controlled and securely stored within designated controlled areas;
- controlled areas designated to physically control and securely store the media;
- security measures to physically control and securely store the media within designated controlled areas;

the organization physically controls and securely stores CMS information system media within organization-defined controlled areas using organization-defined security measures;

the organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

the organization meets all the requirements specified in the applicable 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; security plan; information system media; other relevant documents or records.

**Examine:** Cryptographic software licenses used to protect PII at rest.

**Examine:** PII magnetic media storage procedures.

**Interview:** Organizational personnel with PII protection responsibilities.

**Interview:** Organizational personnel with information system media protection and storage responsibilities.

| MP-5 – Media Transport (High) |
| --- |
| **Control**<br>The organization:<br>a. Protects and controls digital and non-digital media containing CMS sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier;<br>b. Maintains accountability for information system media during transport outside of controlled areas; and<br>c. Restricts the activities associated with transport of such media to authorized personnel.<br>**Implementation Standard(s)**<br>1. (For PII only) Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.<br>2. (For FTI only) Organizations are not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7) |

**Guidance**

Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting CMS information and/or CMS information system.

Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides: (i) the selection of media and associated information contained on that media requiring protection during transport; and (ii) the selection and use of storage containers for transporting non-digital media.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.6#2, 4.6#4 | **Related Controls**<br>**Requirement(s):** AC-19, CP-9, CP-9(4) |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-5.1**

**Assessment Objective**

Determine if:

the organization protects and controls digital and non-digital media containing CMS sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and (a) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier;

the organization maintains accountability for information system media during transport outside of controlled areas;

the organization identifies personnel authorized to transport information system media outside of controlled areas;

the organization restricts the activities associated with transport of information system media to authorized personnel.

the organization meets all the requirements specified in the applicable 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; security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records.

**Examine:** Rosters or list of authorized personnel to protect and control PII media during transit.

**Examine:** FTI disclosure documentation. (See IRS Pub. 1075, sect. 11.1 and 11.7)

**Interview:** Organizational personnel responsible for FTI disclosure.

**Interview:** Organizational personnel with information system media transport responsibilities.

**MP-5(1) – Enhancement (High)**

**Control**

[Withdrawn: Incorporated into MP-5].

**MP-5(2) – Enhancement (High)**

**Control**

The organization documents activities associated with the transport of information system media.

**Guidance**

Organizations establish documentation requirements for activities associated with the transport of CMS information system media in accordance with CMS requirements.

| **Applicability:** All | **Reference(s):** IRS-1075: 3.2#3.1, 4.4#2, 4.6#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-5(2).1**

**Assessment Objective**

Determine if the organization documents activities associated with the transport of information system media.

**Assessment Methods And Objects**

**Examine:** Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media transport records; audit records; other relevant documents or records.

**MP-5(3) – Enhancement (High)**

**Control**

The organization employs an identified custodian throughout the transport of CMS information system media.

**Guidance**

Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

| **Applicability:** All | **Reference(s):** IRS-1075: 4.4#2, 4.6#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-5(3).1**

**Assessment Objective**

Determine if the organization employs an identified custodian throughout the transport of information system media.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system media transport responsibilities.

**MP-5(4) – Enhancement (High)**

**Control**

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

**Guidance**

This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-5(4).1**

**Assessment Objective**

Determine if the organization employs 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; other relevant documents or records.

**Test:** Cryptographic mechanisms protecting information during transportation outside controlled areas.

**MP-6 – Media Sanitization (High)**

**Control**

The organization:
a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

**Implementation Standard(s)**

1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.
2. (For FTI only) FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee.
3. (For PII only) Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:
- date received
- reel/cartridge control number contents
- number of records, if available
- movement, and
- if disposed of, the date and method of disposition.

**Guidance**

This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of sensitive information to unauthorized individuals when such media is reused or released for disposal. The organization uses its discretion on the employment of 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 CMS or individuals if released for reuse or disposal.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-1075: 4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2 | **Related Controls Requirement(s):** MA-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-6.1**

**Assessment Objective**

Determine if:
the organization sanitizes information system media both digital and non-digital prior to:
- disposal;
- release out of organizational control; or
- release for reuse;

the organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records.

**Examine:** FTI disposal records.

**Examine:** PII inventory tape/cartridge log.

**Interview:** Organizational personnel with information system media sanitization responsibilities.

**MP-6(1) – Enhancement (High)**

**Control**

The organization tracks, documents, and verifies media sanitization and disposal actions.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-6(1).1**

**Assessment Objective**

Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.

**Assessment Methods And Objects**

**Examine:** Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system media sanitization responsibilities.

| MP-6(2) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization tests sanitization equipment and procedures to verify correct performance periodically. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-6(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the frequency for testing sanitization equipment and procedures to verify correct performance;<br>the organization tests sanitization equipment and procedures to verify correct performance in accordance with organization-defined frequency.<br>**Assessment Methods And Objects**<br>**Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records.<br>**Interview:** Organizational personnel with information system media sanitization responsibilities. | | |
| **MP-6(3) – Enhancement (High)** | | |
| **Control**<br>The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: (i) prior to initial use after purchase, (ii) when obtained from unknown sources, and (iii) when the organization loses a positive chain of custody. | | |

**Guidance**

Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily transferred to the information system through USB ports or other entry portals. While scanning such devices is always recommended, sanitization provides additional assurance that the device is free of all malicious code to include code capable of initiating zero-day attacks. Organizations consider sanitization of portable, removable storage devices, for example, when such devices are first purchased from the manufacturer or vendor prior to initial use or when the organization loses a positive chain of custody for the device. An organizational assessment of risk guides the specific circumstances for employing the sanitization process.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-6(3).1**

**Assessment Objective**

Determine if:
the organization defines circumstances requiring sanitization of portable, removable storage devices prior to connecting such devices to the information system;

the organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under organization-defined circumstances.

**Assessment Methods And Objects**

**Examine:** Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system media sanitization responsibilities.

**MP-6(5) – Enhancement (High)**

**Control**

The organization sanitizes information system media containing sensitive information using National Security Agency (NSA) guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, Guidelines for Media Sanitization.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-6(5).1**

**Assessment Objective**

Determine if the organization sanitizes information system media containing classified information in accordance with NSA standards and policies.

**Assessment Methods And Objects**

**Examine:** Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system media sanitization responsibilities.

**MP-6(6) – Enhancement (High)**

**Control**

The organization destroys media containing sensitive information that cannot be sanitized.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-6(6).1**

**Assessment Objective**

Determine if the organization implements the media destruction process for information system media that cannot be sanitized.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system media sanitization responsibilities.

**MP-CMS-1 – Media Related Records (High)**

**Control**

Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.

**Implementation Standard(s)**

1. The media records must, at a minimum, contain:
(a) The name of media recipient;
(b) Signature of media recipient;
(c) Date/time media received;
(d) Media control number and contents;
(e) Movement or routing information; and
(f) If disposed of, the date, time, and method of destruction.

**Guidance**

Employing a hash function (a reproducible method of turning inventory data into a relatively small number may serve as a digital "fingerprint" of the data) for electronic inventory records maintenance so the inventory information can be validated as not being tampered with prior to reconstructive events for an investigation of a possible breach.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-CMS-1.1**

**Assessment Objective**

Determine if:
the organization maintains inventory and disposition records for information system media to ensure control and accountability of CMS information;

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Media protection policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with information system media protection responsibilities.

# 11.0 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PE-1 – Physical and Environmental Protection Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-2, CP-2, SM-1, SM-3; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents physical and environmental protection policy; | | |

the organization physical and environmental protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities;

the organization develops and formally documents physical and environmental protection procedures;

the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls;

the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities;

the organization reviews/updates the physical and environmental protection policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with physical and environmental protection responsibilities.

**PE-2 – Physical Access Authorizations (High)**

**Control**

The organization:
a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
b. Issues authorization credentials;
c. Reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.

**Implementation Standard(s)**

1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every ninety (90) days.
2. (For PII only) Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.

**Guidance**

Authorization credentials include, for example, badges, identification cards, and smart cards.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-2.1**

**Assessment Objective**

Determine if:
the organization identifies areas within the facility that are publicly accessible;

the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

the organization issues authorization credentials (e.g., badges, identification cards, smart cards).

the organization reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** Restricted areas, security rooms, or locked rooms that control access to areas containing PII.

**Interview:** Organization personnel responsible for controlling restricted areas, security rooms, or locked rooms containing PII.

| PE-3 – Physical Access Control (High) |
|---|
| **Control**<br>The organization:<br>a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);<br>b. Verifies individual access authorizations before granting access to the facility;<br>c. Controls entry to the facility containing the information system using physical access devices and/or guards;<br>d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;<br>e. Controls access authorization lists to secure areas;<br>f. Secures keys, combinations, and other physical access devices;<br>g. Inventories physical access devices within every three hundred sixty-five (365) days; and<br>h. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.<br>**Implementation Standard(s)**<br>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.<br>2. Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.<br>3. Restrict access to grounds/facilities to authorized persons only.<br>4. (For PII only) 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 after hours. |
| **Guidance**<br>The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) a CMS information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SD-1, SM-4; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-3.1**

**Assessment Objective**

Determine if:
the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

the organization verifies individual access authorizations before granting access to the facility;

the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;

the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

the organization secures keys, combinations, and other physical access devices;

the organization inventories physical access devices within every three hundred sixty-five (365) days;

the organization changes combinations and keys periodically; and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** PII protection barriers.

**Interview:** Organizational personnel with physical access control responsibilities.

**Test:** Physical access control capability; physical access control devices.

**PE-3(1) – Enhancement (High)**

**Control**

The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.

**Guidance**

the organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.

| **Applicability:** All | **Reference(s):** IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-3(1).1**

**Assessment Objective**

Determine if the organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.

**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; other relevant documents or records.

## PE-4 – Access Control for Transmission Medium (High)

**Control**

The organization controls physical access to information system distribution and transmission lines within organizational facilities.

**Implementation Standard(s)**

1. Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel.
2. Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use.

**Guidance**

Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-4.1**

**Assessment Objective**

Determine if:
the organization controls physical access to information system distribution and transmission lines within organizational facilities.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PE-5 – Access Control for Output Devices (High)**

**Control**

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

**Guidance**

Monitors, printers, and audio devices are examples of information system output devices.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6; HIPAA: 164.310(b) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-5.1**

**Assessment Objective**

Determine if the organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; actual displays from information system components; other relevant documents or records.

| PE-6 – Monitoring Physical Access (High) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Monitors physical access to the information system to detect and respond to physical security incidents;<br>b. Reviews physical access logs in accordance with the frequency specified in Implementation Standard 1; and<br>c. Coordinates results of reviews and investigations with the organization's incident response capability.<br>**Implementation Standard(s)**<br>1. Review physical access logs every at least once every month. | | |
| **Guidance**<br>Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AC-6, SM-5 | **Related Controls Requirement(s):** IR-4 |
| **ASSESSMENT PROCEDURE: PE-6.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization monitors physical access to the information system to detect and respond to physical security incidents;<br>the organization reviews physical access logs in accordance with the organization-defined frequency;<br>the organization coordinates results of reviews and investigations with the organization's incident response capability.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**Examine:** Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical access logs or records; other relevant documents or records.<br>**Interview:** Organizational personnel with physical access monitoring responsibilities.<br>**Test:** Physical access monitoring capability. | | |

| PE-6(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization monitors real-time physical intrusion alarms and surveillance equipment. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-6(1).1** | | |
| **Assessment Objective**<br>Determine if the organization monitors real-time physical intrusion alarms and surveillance equipment.<br>**Assessment Methods And Objects**<br>**Examine:** Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; other relevant documents or records.<br>**Interview:** Organizational personnel with physical access monitoring responsibilities.<br>**Test:** Physical access monitoring capability. | | |
| **PE-6(2) – Enhancement (High)** | | |
| **Control**<br>The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-6(2).1** | | |
| **Assessment Objective**<br>Determine if the organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.<br>**Assessment Methods And Objects**<br>**Examine:** Physical and environmental protection policy; procedures addressing physical access monitoring; information system design documentation; other relevant documents or records.<br>**Test:** Automated mechanisms implementing physical access monitoring capability. | | |

| PE-7 – Visitor Control (High) | | |
|---|---|---|
| **Control**<br>The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. | | |
| **Guidance**<br>Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6; HIPAA: 164.310(a)(2)(iii) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-7.1** | | |
| **Assessment Objective**<br>Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.<br>**Assessment Methods And Objects**<br>**Examine:** Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.<br>**Interview:** Organizational personnel with visitor access control responsibilities.<br>**Test:** Visitor access control capability. | | |
| **PE-7(1) – Enhancement (High)** | | |
| **Control**<br>The organization escorts visitors and monitors visitor activity, when required. | | |
| **Applicability:** All | **Reference(s):** HIPAA: 164.310(a)(2)(iii) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-7(1).1** | | |
| **Assessment Objective**<br>Determine if the organization escorts visitors and monitors visitor activity, when required. | | |

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.

**Interview:** Organizational personnel with visitor access control responsibilities.

**PE-8 – Access Records (High)**

**Control**

The organization:
a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
b. Closes and reviews visitor access records monthly.

**Guidance**

Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-8.1**

**Assessment Objective**

Determine if:
the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

the organization reviews the visitor access records in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for reviewing physical access records.

**PE-8(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to facilitate the maintenance and review of access records.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-8(1).1**

**Assessment Objective**

Determine if the organization maintains a record of all physical access, both visitor and authorized individuals.

**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; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for reviewing physical access records.

**PE-8(2) – Enhancement (High)**

**Control**

The organization maintains a record of all physical access, both visitor and authorized individuals.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-8(2).1**

**Assessment Objective**

Determine if the organization maintains a record of all physical access, both visitor and authorized individuals.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing facility access records; facility access control logs or records; other relevant documents or records.

**PE-9 – Power Equipment and Power Cabling (High)**

**Control**

The organization protects power equipment and power cabling for the information system from damage and destruction.

**Implementation Standard(s)**

1. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-9.1**

**Assessment Objective**

Determine if:
the organization protects power equipment and power cabling for the information system from damage and destruction.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PE-10 – Emergency Shutoff (High)**

**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;
c. Protects emergency power shutoff capability from unauthorized activation; and
d. 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.

**Guidance**

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

| **Applicability:** All | **Reference(s):** FISCAM: CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-10.1**

**Assessment Objective**

Determine if:
the organization provides the capability of shutting off power to the information system or individual system components in emergency situations;

the organization defines the location of emergency shutoff switches or devices by information system or system component;

the organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel;

the organization protects the emergency power shutoff capability from unauthorized activation.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; other relevant documents or records.

**PE-10(1) – Enhancement (High)**

**Control**

[Withdrawn: Incorporated into PE-10].

**PE-11 – Emergency Power (High)**

**Control**

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-11.1**

**Assessment Objective**

Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; other relevant documents or records.

**Test:** Uninterruptible power supply.

**PE-11(1) – Enhancement (High)**

**Control**

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-11(1).1**

**Assessment Objective**

Determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records.

**Test:** Alternate power supply.

**PE-12 – Emergency Lighting (High)**

**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 that covers emergency exits and evacuation routes within the facility.

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-12.1**

**Assessment Objective**

Determine if:

the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption;

the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility;

the organization maintains the automatic emergency lighting for the information system.

**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; other relevant documents or records.

**Interview:** Organizational personnel with emergency planning responsibilities.

**Test:** Emergency lighting capability.

**PE-13 – Fire Protection (High)**

**Control**

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

**Guidance**

Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13.1**

**Assessment Objective**

Determine if:
the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source;

the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

**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; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems.

**PE-13(1) – Enhancement (High)**

**Control**

The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13(1).1**

**Assessment Objective**

Determine if the organization employs fire detection devices/systems for the information system that, without manual intervention, activate automatically and notify the organization and emergency responders in the event of a fire.

**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; 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) – Enhancement (High)**

**Control**

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13(2).1**

**Assessment Objective**

Determine if the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems.

**Test:** Simulated activation of fire suppression devices/systems and automated notifications.

**PE-13(3) – Enhancement (High)**

**Control**

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13(3).1**

**Assessment Objective**

Determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

**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; 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-14 – Temperature and Humidity Controls (High)

**Control**

The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and
b. Monitors temperature and humidity levels.

**Implementation Standard(s)**

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

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-14.1**

**Assessment Objective**

Determine if:
the organization defines the acceptable temperature and humidity levels within the facility where the information system resides;

the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels;

the organization defines the frequency to monitor temperature and humidity levels;

the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PE-15 – Water Damage Protection (High)**

**Control**

The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-15.1**

**Assessment Objective**

Determine if:
the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly;

key personnel within the organization have knowledge of the master water shutoff values.

**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; 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) – Enhancement (High)**

**Control**

The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-15(1).1**

**Assessment Objective**

Determine if the organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.

**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; other relevant documents or records.

**Test:** Automated mechanisms implementing master water shutoff valve activation.

**PE-16 – Delivery and Removal (High)**

**Control**

The organization authorizes, monitors, and controls the flow of CMS information system-related components entering and exiting the facility and maintains records of those items.

**Guidance**

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: PE-16.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility;<br>the organization maintains records of information system components entering and exiting the facility.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Interview:** Organization personnel with responsibilities for controlling information system components entering and exiting the facility.<br>**Test:** Process for controlling information system-related items entering and exiting the facility. | | |
| **PE-17 – Alternate Work Site (High)** | | |
| **Control**<br>The organization:<br>a. Employs appropriate security controls at alternate work sites to include, but not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems;<br>b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and<br>c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. | | |
| **Guidance**<br>Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites. | | |
| **Applicability:** All | **Reference(s):** FISCAM: CP-2; HIPAA: 164.310(a)(2)(i) | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: PE-17.1**

**Assessment Objective**

Determine if:
the organization defines the management, operational, and technical information system security controls to be employed at alternate work sites;

the organization employs organization-defined management, operational, and technical information system security controls at alternate work sites;

the organization assesses, as feasible, the effectiveness of security controls at alternate work sites;

the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.

**Assessment Methods And Objects**

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

**Interview:** Organization personnel using alternate work sites.

**PE-18 – Location of Information System Components (High)**

**Control**

The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

**Guidance**

Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2; HIPAA: 164.312(c)(1) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-18.1**

**Assessment Objective**

Determine if:
the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards;

the organization positions information system components within the facility to minimize the opportunity for unauthorized access.

**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; other relevant documents or records.

**PE-18(1) – Enhancement (High)**

**Control**

The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-18(1).1**

**Assessment Objective**

Determine if:
the organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards;

the organization, for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; physical site planning documents; organizational assessment of risk, contingency plan; other relevant documents or records.

**Interview:** Organization personnel with site selection responsibilities for the facility housing the information system.

# 12.0 PLANNING (PL) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PL-1 – Security Planning Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PL-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security planning policy; | | |

the organization security planning policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities;

the organization develops and formally documents security planning procedures;

the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls;

the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities;

the organization reviews/updates the security planning policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Security planning policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with security planning responsibilities.

## PL-2 – System Security Plan (SSP) (High)

**Control**

The organization:
a. Develops a security plan for the information system that:
- Is consistent with the CMS System Security Plan (SSP) Procedure;
- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the operational environment for the information system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and
c. 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 due to changes in the threat environment; or
- Before the previous security authorization expires.

**Implementation Standard(s)**

1. (For PHI only) 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).)
2. (For FTI only) When FTI is incorporated into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition to those specified in other controls.
3. (For FTI only) Develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7 & 8)

**Guidance**

The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to CMS operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended.

All CMS information systems and major applications are covered by an SSP, which is compliant with current CMS SSP Procedures.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, CP-1, CP-2, SM-1; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PL-2.1**

**Assessment Objective**

Determine if:
the organization develops a security plan for the information system that:
- is consistent with the organization's enterprise architecture;
- explicitly defines the authorization boundary for the system;
- describes the operational context of the information system in terms of mission and business processes;
- provides the security categorization of the information system including supporting rationale;
- describes the operational environment for the information system;
- describes relationships with or connections to other information systems;
- provides an overview of the security requirements for the system;
- describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions;
- is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

the organization defines the frequency of security plan reviews;

the organization reviews the security plan in accordance with the organization-defined frequency, minimally every three (3) years;

the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** Sampling of policies and procedures relating to 164.306 for retention period. (See HIPAA 164.316(b))

**Examine:** Compliance controls if FTI is incorporated into a Data Warehouse. (See IRS Pub 1075 Exhibit 7)

**Examine:** SPRs and SARs..

**Examine:** Procedures that document who obtains documentation and which documentation pertains to whom for implementation.

**Interview:** Organization personnel with security planning and plan implementation responsibilities for the information system.

**Interview:** Organizational personnel with retention responsibilities related to 164.306. (See HIPAA 164.316(b))

**Interview:** Organizational personnel who are responsible for implementation of procedures to determine if documentation is available.

**PL-3 – System Security Plan Update (High)**

**Control**

[Withdrawn: Incorporated into PL-2].

**PL-4 – Rules of Behavior (ROB) (High)**

**Control**

The organization:
a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information, information system, and network use; and
b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

**Guidance**

The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior.
ROBs are aligned with DHHS requirements posted at http://hhs.gov/ocio/policy/2008-0001.003s.html, and made readily available.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, SM-4; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PL-4.1**

**Assessment Objective**

Determine if:
the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;

the organization makes the rules available to all information system users;

the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

**Assessment Methods And Objects**

**Examine:** Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records.

**Interview:** Organizational personnel who are authorized users of the information system and have signed rules of behavior.

**PL-5 – Privacy Impact Assessment (PIA) (High)**

**Control**

The organization conducts a Privacy Impact Assessment (PIA) on the information system in accordance with OMB policy.

| | | |
|---|---|---|
| **Applicability:** All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC | **Reference(s):** FISCAM: SM-5; HSPD 7: J(35) | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: PL-5.1**

**Assessment Objective**

Determine if:
the organization conducts a privacy impact assessment on the information system;

the privacy impact assessment is in accordance with OMB policy.

**Assessment Methods And Objects**

**Examine:** Security planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records.

**PL-6 – Security-Related Activity Planning (High)**

**Control**

The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on CMS operations (i.e., mission, functions, image, and reputation), CMS assets, and individuals.

**Guidance**

Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.

| **Applicability:** All | **Reference(s):** FISCAM: SM-1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PL-6.1**

**Assessment Objective**

Determine if the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

**Assessment Methods And Objects**

**Examine:** Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records.

**Interview:** Organizational personnel with security planning and plan implementation responsibilities.

# 13.0 PERSONNEL SECURITY (PS) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PS-1 – Personnel Security Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SD-2, SM-1, SM-3, SM-4; IRS-1075: 5.6.2.1#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PS-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents personnel security policy; | | |

the organization personnel security policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities;

the organization develops and formally documents personnel security procedures;

the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls;

the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities;

the organization reviews/updates the personnel security policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Personnel security policy and procedures, other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

**PS-2 – Position Categorization (High)**

**Control**

The organization:
a. Assigns a criticality/sensitivity risk designation to all positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and revises position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.

**Guidance**

Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).

| **Applicability:** All | **Reference(s):** FISCAM: SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-2.1**

**Assessment Objective**

Determine if:
the organization assigns a risk designations to all positions within the organization;

the organization establishes a screening criteria for individuals filling organizational positions;

the organization defines in the security plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions;

the organization reviews/revises position risk designations within every three hundred sixty-five (365) days.

**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; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

**PS-3 – Personnel Screening (High)**

**Control**

The organization:
a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position.

**Implementation Standard(s)**

1. Perform criminal history check for all persons prior to employment.
2. Require appropriate personnel to obtain and hold a high-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook.

**Guidance**

Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. For prospective employees, references background checks are performed before issuance of a User ID. Security agreements are required for employees and contractors assigned to work with mission critical information.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SM-4, SM-7; IRS-1075: 5.6.2.1#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-3.1**

**Assessment Objective**

Determine if:
the organization screens individuals prior to authorizing access to the information system;

the organization rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position;

the personnel screening is consistent with 5 CFR 731.106, OPM policy, regulations, and guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

**PS-4 – Personnel Termination (High)**

**Control**

The organization, upon termination of individual employment:
a. Revokes system and physical access immediately following employee termination;
b. Conducts exit interviews;
c. Retrieves all security-related CMS information system-related property;
d. Retains access to CMS information and information systems formerly controlled by terminated individual; and
e. Immediately escorts employees terminated for cause out of the organization.

**Implementation Standard(s)**

1. System access must be revoked prior to or during the employee termination process.

**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 individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all CMS information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and non-availability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause. Appropriate personnel have access to official records created by the terminated employee that are stored on CMS information systems.

| **Applicability:** All | **Reference(s):** FISCAM: SM-4; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: 5.6.2.1#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-4.1**

**Assessment Objective**

Determine if:

the organization terminates information system access upon termination of individual employment;

the organization conducts exit interviews of terminated personnel;

the organization retrieves all security-related CMS information system-related property from terminated personnel;

the organization, upon termination of individual employment, retrieves all security-related CMS information system-related property;

the organization, upon termination of individual employment, retains access to CMS information and information systems formerly controlled by terminated individual;

the organization, upon termination of individual employment, immediately escorts employees terminated for cause out of the organization.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

| PS-5 – Personnel Transfer (High) | | |
|---|---|---|
| **Control**<br>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 the following transfer or reassignment actions during the formal transfer process:<br>a. Re-issuing appropriate CMS information system-related property (e.g., keys, identification cards, building passes);<br>b. Notification to security management;<br>c. Closing obsolete accounts and establishing new accounts; and<br>d. Revocation of all system access privileges (if applicable). | | |
| **Guidance**<br>This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts. | | |
| **Applicability:** All | **Reference(s):** FISCAM: SM-4; IRS-1075: 5.6.2.1#1.6 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PS-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization;<br>the organization defines the transfer or reassignment actions and the time period within which the actions must occur following formal transfer or reassignment;<br>the organization initiates the organization-defined transfer or reassignment actions within an organization-defined time period following formal transfer or reassignment. | | |

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

**PS-6 – Access Agreements (High)**

**Control**

The organization:
a. Ensures that individuals requiring access to CMS information or information systems sign appropriate access agreements prior to being granted access; and
b. Reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended.

**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 the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-6.1**

**Assessment Objective**

Determine if:
the organization identifies appropriate access agreements for individuals requiring access to CMS information and information systems;

individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access;

the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates for access agreements;

the organization reviews/updates the access agreements in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with personnel security responsibilities.

**PS-7 – Third-Party Personnel Security (High)**

**Control**

The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Documents personnel security requirements; and
c. Monitors provider compliance.

**Implementation Standard(s)**

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 CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies and standards.

**Guidance**

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. Security requirements include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SD-1, SM-4, SM-7; IRS-1075: 5.6.2.1#1.8 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-7.1**

**Assessment Objective**

Determine if:
the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers;

the organization documents personnel security requirements for third-party providers;

the organization monitors third-party provider compliance with personnel security requirements.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities; third-party providers.

**PS-8 – Personnel Sanctions (High)**

**Control**

The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

**Guidance**

The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, SD-2, SM-4; HIPAA: 164.308(a)(1)(ii)(C) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-8.1**

**Assessment Objective**

Determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with personnel security responsibilities.

# 14.0 RISK ASSESSMENT (RA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **RA-1 – Risk Assessment Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-2, SM-3; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075: 5.6.1.1#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: RA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents risk assessment policy; | | |

the organization risk assessment policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities;

the organization develops and formally documents risk assessment procedures;

the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls;

the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities;

the organization reviews/updates the risk assessment policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with risk assessment responsibilities.

**RA-2 – Security Categorization (High)**

**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 designated representative.

**Guidance**

A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to CMS operations, CMS assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the CMS CIO, CISO, Business Owner, senior information security officer, and information owners/stewards. The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted.
All CMS information systems categorized as High or Moderate are considered sensitive or to contain sensitive information. All CMS information systems categorized as Low are considered non-sensitive or to 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.

| **Applicability:** All | **Reference(s):** FISCAM: CP-1, SM-2; HSPD 7: D(8); IRS-1075: 4.1#2 | **Related Controls Requirement(s):** MP-4, SC-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-2.1**

**Assessment Objective**

Determine if:
the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

the organization documents the security categorization results (including supporting rationale) in the security plan for the information system;

the CMS authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

**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; other relevant documents or records.

**Interview:** Organizational personnel with security categorization and risk assessment responsibilities.

| RA-3 – Risk Assessment (High) |
|---|
| **Control**<br>The organization:<br>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;<br>b. Documents risk assessment results in accordance with the CMS Information Security (IS) Risk Assessment (RA) Procedures;<br>c. Reviews risk assessment results within every three hundred sixty-five (365) days; and<br>d. Updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. |
| **Guidance**<br>A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to CMS operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to CMS operations, CMS assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing CMS information systems, outsourcing entities).<br>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. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems.<br>Risk assessments can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the baselines with additional security controls or control enhancements. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-5, CP-1, CP-2, SM-2; HIPAA: 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3, 6.3.3#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-3.1**

**Assessment Objective**

Determine if:
the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:
- access;
- use;
- disclosure;
- disruption;
- modification; or
- destruction;

the organization documents risk assessment results in accordance with the CMS IS RA Procedures;

the organization reviews risk assessment results within every three hundred sixty-five (365) days;

the organization updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records.

**Interview:** Organizational personnel with risk assessment responsibilities.

**RA-4 – Risk Assessment Update (High)**

**Control**

[Withdrawn: Incorporated into RA-3].

| RA-5 – Vulnerability Scanning (High) |
|---|
| **Control**<br>The organization:<br>a. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:<br>- Enumerating platforms, software flaws, and improper configurations;<br>- Formatting and making transparent, checklists and test procedures; and<br>- Measuring vulnerability impact;<br>b. Analyzes vulnerability scan reports and results from security control assessments;<br>c. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and<br>d. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).<br>**Implementation Standard(s)**<br>1. Scans for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported.<br>2. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with CMS IS procedures. |
| **Guidance**<br>The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan. |

| **Applicability:** All | **Reference(s):** FISCAM: CM-5, SM-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5.1**

**Assessment Objective**

Determine if:
the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:
- enumerating platforms, software flaws, and improper configurations;
- formatting/and making transparent checklists and test procedures;
- measuring vulnerability impact;

the organization analyzes vulnerability scan reports and results from security control assessments;

the organization remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk;

the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.

**Interview:** Organizational personnel with risk assessment and vulnerability scanning responsibilities.

**RA-5(1) – Enhancement (High)**

**Control**

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

| **Applicability:** All | **Reference(s):** HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5(1).1**

**Assessment Objective**

Determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; records of updates to vulnerabilities scanned; other relevant documents or records.

**Test:** Vulnerability scanning capability and associated scanning tools.

**RA-5(2) – Enhancement (High)**

**Control**

The organization updates the list of information system vulnerabilities scanned within every three hundred sixty-five (365) days or when new vulnerabilities are identified and reported.

| | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24) | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: RA-5(2).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the frequency of updates for information system vulnerabilities scanned;

the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when new vulnerabilities are identified and reported.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records.

**RA-5(3) – Enhancement (High)**

**Control**

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

| **Applicability:** All | **Reference(s):** HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5(3).1**

**Assessment Objective**

Determine if:
the organization employs vulnerability scanning procedures that can demonstrate the breadth of coverage (i.e., information system components scanned);

the organization employs vulnerability scanning procedures that can demonstrate the depth of coverage (i.e., vulnerabilities checked).

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and information system components checked; other relevant documents or records.

**RA-5(4) – Enhancement (High)**

**Control**

The organization attempts to discern what information about the information system is discoverable by adversaries.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5(4).1**

**Assessment Objective**

Determine if the organization attempts to discern what information about the information system is discoverable by adversaries.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; penetration test results; vulnerability scanning results; other relevant documents or records.

**RA-5(5) – Enhancement (High)**

**Control**

The organization includes privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5(5).1**

**Assessment Objective**

Determine if:
the organization defines the list of information system components to which privileged access is authorized for selected vulnerability scanning activities;

the organization includes privileged access authorization to organization-defined information system components identified for selected vulnerability scanning activities to facilitate more thorough scanning.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; security plan; list of information system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; other relevant documents or records.

**RA-5(7) – Enhancement (High)**

**Control**

The organization employs automated mechanisms no less than quarterly to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5(7).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms no less than quarterly to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; security plan; information system design documentation; list of unauthorized software; notifications or alerts of unauthorized software on organizational information systems; other relevant documents or records.

**Test:** Vulnerability scanning capability and associated scanning tools.

| RA-5(9) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization employs an independent penetration agent or penetration team to:<br>(a) Conduct a vulnerability analysis on the information system; and<br>(b) Perform internal/external penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities. | | |
| **Guidance**<br>A standard method for penetration testing includes: (i) pre-test analysis based on full knowledge of the target information system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: RA-5(9).1** | | |
| **Assessment Objective**<br>Determine if the organization employs an independent penetration agent or penetration team to:<br>- conduct a vulnerability analysis on the information system;<br>- perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.<br>**Assessment Methods And Objects**<br>**Examine:** Risk assessment policy; security assessment policy; procedures addressing vulnerability analysis; risk assessment; security plan; other relevant documents or records.<br>**Interview:** Organizational personnel with vulnerability scanning and analysis responsibilities. | | |

# 15.0 SYSTEM AND SERVICES ACQUISITION (SA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| SA-1 – System and Services Acquisition Policy and Procedures (High) |
|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.<br>**Implementation Standard(s)**<br>1. (For FTI only) Develop, disseminates, and periodically reviews/updates a formal, documented, system and services acquisition policy that includes IRS documents received and identified by:<br>(a) Taxpayer name<br>(b) Tax year(s)<br>(c) Type of information (e.g., revenue agent reports, Form 1040, work papers)<br>(d) The reason for the request<br>(e) Date requested<br>(f) Date received<br>(g) Exact location of the FTI<br>(h) Who has had access to the data and<br>(i) If disposed of, the date and method of disposition. |

**Guidance**

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.1.3#1.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-1.1**

**Assessment Objective**

Determine if:

the organization develops and formally documents system services and acquisition policy;

the organization system services and acquisition policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system services and acquisition policy to elements within the organization having associated system services and acquisition roles and responsibilities;

the organization develops and formally documents system services and acquisition procedures;

the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls;

the organization disseminates formal documented system services and acquisition procedures to elements within the organization having associated system services and acquisition roles and responsibilities;

the organization reviews/updates the system services and acquisition policy and procedures within every three hundred sixty-five (365) days.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** System and services acquisition policy and procedures; other relevant documents or records.

**Examine:** Organizational documentation that contains the development, dissemination, and review/updates to FTI IRS documents received.

**Interview:** Organizational personnel with system and services acquisition responsibilities.

## SA-2 – Allocation of Resources (High)

**Control**

The organization:
a. Includes a determination of information security requirements for the information system in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system 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' programming and budgeting documentation for the implementation and management of information systems security.

| **Applicability:** All | **Reference(s):** FISCAM: CM-3, IN-2, SD-1, SM-1 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: SA-2.1

**Assessment Objective**

Determine if:
the organization includes a determination of the information security requirements for the information system in mission/business process planning;

the organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process;

the organization establishes a discrete line item for information security in organizational programming and budgeting documentation;

the organization establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security.

**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 – Life Cycle Support (High)**

**Control**

The organization:
a. Manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS Integrated IT Investment & System Life Cycle Framework (ILC);
b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
c. Identifies individuals having information system security roles and responsibilities.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-3, AS-5, BP-1, BP-2, BP-3, BP-4, CM-1, CM-3, CP-3, DA-1, IN-1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-3.1**

**Assessment Objective**

Determine if:
the organization manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS Integrated IT Investment & System Life Cycle Framework (ILC);

the organization defines and documents information system security roles and responsibilities throughout the system development life cycle;

the organization identifies individuals having information system security roles and responsibilities.

**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 – Acquisitions (High)**

**Control**

The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
a. Security functional requirements/specifications;
b. Security-related documentation requirements; and
c. Developmental and evaluation-related assurance requirements.

**Implementation Standard(s)**

1. Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

**Guidance**

The acquisition documents for CMS information systems, CMS information system components, and CMS information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.

Solicitation Documents:

Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required:

- Security capabilities;
- Design and development processes;
- Test and evaluation procedures; and
- Documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

Use of Evaluated and Validated Products:

For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources:

1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-3, SM-7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-4.1**

**Assessment Objective**

Determine if:
the organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
- security functional requirements/specifications;
- security-related documentation requirements;
- developmental and evaluation-related assurance requirements.

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 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) – Enhancement (High)**

**Control**

The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-4(1).1**

**Assessment Objective**

Determine if the organization requires in acquisition documents that vendors/contractors provide information describing in the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.

**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) – Enhancement (High)**

**Control**

The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-4(2).1**

**Assessment Objective**

Determine if the organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.

**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(4) – Enhancement (High)**

**Control**

The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-4(4).1**

**Assessment Objective**

Determine if:
the organization explicitly assigns each acquired information system component to an information system;
the owner of the system acknowledges each assignment of information system components to the information system.

**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; information system owner.

**SA-5 – Information System Documentation (High)**

**Control**

The organization:
a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
- Secure configuration, installation, and operation of the information system;
- Effective use and maintenance of security features/functions; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and
b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
- User-accessible security features/functions and how to effectively use those security features/functions;
- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
- User responsibilities in maintaining the security of the information and information system; and
c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

**Implementation Standard(s)**

1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.
2. Maintain an updated list of related system operations and security documentation.
3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation.

**Guidance**

The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, AS-3, AS-4, AS-5, BP-1, BP-2, BP-3, BP-4, CM-2, CM-3, CP-2, DA-1, IN-1, IN-2, SD-1, SD-2; IRS-1075: 5.6.1.3#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-5.1**

**Assessment Objective**

Determine if:
the organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
- secure configuration, installation, and operation of the information system;
- effective use and maintenance of the security features/functions;
- known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

the organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
- user-accessible security features/functions and how to effectively use those security features/functions;
- methods for user interaction with the information system, which enables individuals to use the system in a more secure manner;
- user responsibilities in maintaining the security of the information and information system;

the organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

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 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.

**ASSESSMENT PROCEDURE: SA-5.FIS-1**

**Assessment Objective**

Determine if:
the organization develops information system documentation for operating the system that includes:
- operational instructions and
- appropriate end user control, balancing, and verification features and procedures.

the organization disseminates information system documentation to appropriate elements within the organization;

responsible parties within the organization periodically review information system documentation;

the organization updates information system documentation when organizational review indicates updates are required or changes are made to the system.

**Assessment Methods And Objects**

**Examine:** Information system documentation; other relevant documents or records.

**Interview:** Organizational management and personnel with information system operations, control, and user responsibilities.

**SA-5(1) – Enhancement (High)**

**Control**

The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-5(1).1**

**Assessment Objective**

Determine if:
the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation;

the documentation describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

**Assessment Methods And Objects**

**Examine:** System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records.

**Interview:** Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system.

**SA-5(2) – Enhancement (High)**

**Control**

The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-5(2).1**

**Assessment Objective**

Determine if:
the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation;

the documentation describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.

**Assessment Methods And Objects**

**Examine:** System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records.

**Interview:** Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.

**SA-5(3) – Enhancement (High)**

**Control**

The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

**Guidance**

An information system can be partitioned into multiple subsystems.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-5(3).1**

**Assessment Objective**

Determine if:
the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation;

the documentation describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

**Assessment Methods And Objects**

**Examine:** System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records.

**Interview:** Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system.

| SA-6 – Software Usage Restrictions (High) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Uses software and associated documentation in accordance with contract agreements and copyright laws;<br>b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and<br>c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. | | |
| **Guidance**<br>Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization. | | |
| **Applicability:** All | **Reference(s):** FISCAM: CM-3, CM-5; IRS-1075: 4.7.3#1.2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-6.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization uses software and associated documentation in accordance with contract agreements and copyright laws;<br>the organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution;<br>the organization 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. | | |
| **Assessment Methods And Objects**<br>**Examine:** System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records.<br>**Interview:** Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system. | | |

| SA-7 – User-Installed Software (High) | | |
|---|---|---|
| **Control**<br>The organization prohibits users from downloading or installing software, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, explicit rules govern the installation of software by users.<br>**Implementation Standard(s)**<br>1. If user installed software is authorized, ensure that business rules and technical controls enforce the documented authorizations and prohibitions. | | |
| **Guidance**<br>If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). | | |
| **Applicability:** All | **Reference(s):** FISCAM: CM-3, CM-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users;<br>the organization (or information system) enforces explicit rules governing the installation of software by users.<br>the organization meets all the requirements specified in the applicable implementation standard(s). | | |
| **Assessment Methods And Objects**<br>**Examine:** System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records.<br>**Interview:** Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.<br>**Test:** Enforcement of rules for user installed software on the information system; information system for prohibited software. | | |

| SA-8 – Security Engineering Principles (High) | | |
|---|---|---|
| **Control**<br>The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. | | |
| **Guidance**<br>The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of 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 into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions. | | |
| **Applicability:** All | **Reference(s):** FISCAM: BP-2, BP-4, CM-3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-8.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization applies information system security engineering principles in the specification of the information system;<br>the organization applies information system security engineering principles in the design of the information system;<br>the organization applies information system security engineering principles in the development of the information system;<br>the organization applies information system security engineering principles in the implementation of the information system;<br>the organization applies information system security engineering principles in the modification of the information system. | | |

**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)**

**Control**

The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Monitors security control compliance by external service providers.
d. Prohibits service providers from outsourcing any system function outside the U.S. or its territories.

**Implementation Standard(s)**

1. (For PHI only) A covered entity under HIPAA may permit a business associate to 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. (See HIPAA 164.308(b) and 164.314(a).)

**Guidance**

An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization 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 to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-7; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4 | **Related Controls Requirement(s):** CA-3 |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-9.1**

**Assessment Objective**

Determine if:

the organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services;

the organization monitors security control compliance by external service providers.

the organization prohibits service providers from outsourcing any system function outside the U.S. or its territories.

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; other relevant documents or records.

**Examine:** Business associate assurance documentation. (See HIPAA 164.308(b) and 164.314(a))

**Interview:** Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

**Interview:** Organizational personnel responsible for maintaining business associate assurance documentation. (See HIPAA 164.308(b) and 164.314(a))

## SA-10 – Developer Configuration Management (High)

**Control**

The organization requires that information system developers/integrators:
a. Perform configuration management during information system design, development, implementation, and operation;
b. Manage and control changes to the information system;
c. Implement only organization-approved changes;
d. Document approved changes to the information system; and
e. Track security flaws and flaw resolution.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-3, BP-2, BP-4, CM-3, CM-4, CM-6, CP-2, DA-1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-10.1**

**Assessment Objective**

Determine if:
the organization requires that information system developers/integrators:

perform configuration management during information system:
- design;
- development;
- implementation;
- operation;

manage and control changes to the information system during:
- design;
- development;
- implementation;
- modification;

implement only organization-approved changes;

document approved changes to the information system;

track security flaws and flaw resolution.

**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 (High)**

**Control**

The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):
a. Create and implement a security test and evaluation plan in accordance with, but not limited to the, current CMS procedures;
b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security control assessment process; and
c. Document the results of the security control assessment and flaw remediation processes.

**Implementation Standard(s)**

1. If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results.
2. Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.

**Guidance**

Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-3, CM-3, SM-5 | **Related Controls Requirement(s):** CA-2, CA-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-11.1**

**Assessment Objective**

Determine if:
the organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):
- create and implement a security test and evaluation plan in accordance with, but not limited to the, current CMS procedures;
- implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
- document the results of the security testing/evaluation and flaw remediation processes.

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 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-12 – Supply Chain Protection (High) | | |
|---|---|---|
| **Control**<br>The organization protects against supply chain threats by employing best practices and methodologies that promote integrity, security, and reliability in hardware and software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development as part of a comprehensive, defense-in-breadth information security strategy. | | |
| **Guidance**<br>A defense-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-12.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the measures to be employed to protect against supply chain threats;<br>the organization protects against supply chain threats by employing organization-defined measures as part of a comprehensive, defense-in-breadth information security strategy. | | |
| **Assessment Methods And Objects**<br>**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-13 – Trustworthiness (High)** | | |
| **Control**<br>The organization requires that the information system meet the level of trustworthiness that is sufficient to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. | | |

**Guidance**

The intent of this control is to ensure that organizations recognize the importance of trustworthiness and making explicit trustworthiness decisions when designing, developing, and implementing organizational information systems. Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Two factors affecting the trustworthiness of an information system include: (i) security functionality (i.e., the security features or functions employed within the system); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application).

Appropriate security functionality for the information system can be obtained by using the Risk Management Framework (Steps 1, 2, and 3) to select and implement the necessary management, operational, and technical security controls necessary to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Appropriate security assurance can be obtained by: (i) the actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the system development life cycle. For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of the ongoing monitoring of security controls. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits. Minimum assurance requirements are described in NIST SP 800-53, Revision 3, Appendix E, Minimum Assurance Requirements.

Explicit trustworthiness decisions highlight situations where achieving the information system resilience and security capability necessary to withstand cyber attacks from adversaries with certain threat capabilities may require adjusting the risk management strategy, the design of mission/business processes with regard to automation, the selection and implementation rigor of management and operational protections, or the selection of information technology components with higher levels of trustworthiness. Trustworthiness may be defined on a component-by-component, subsystem-by-subsystem, or function-by-function basis. It is noted, however, that typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and at a minimum, something that likely requires careful attention in order to achieve practically useful results.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-13.1**

**Assessment Objective**

Determine if:
the organization defines the organization's level of trustworthiness;

the organization requires that the information system meet the organization-defined level of trustworthiness.

**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; penetration test and vulnerability scan reports; security test and evaluation results; authority to operate documentation; other relevant documents or records.

**Interview:** Organizational personnel with system and services acquisition responsibilities; information system authorizing official.

# 16.0 SYSTEM AND COMMUNICATIONS PROTECTION (SC) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **SC-1 – System and Communications Protection Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-5, SM-1, SM-3; IRS-1075: 5.6.3.4#1, 5.6.3.4#2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system and communications protection policy; | | |

the organization system and communications protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities;

the organization develops and formally documents system and communications protection procedures;

the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls;

the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities;

the organization reviews/updates the system and communications protection policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with system and communications protection responsibilities.

**SC-2 – Application Partitioning (High)**

**Control**

The information system separates user functionality (including user interface services [e.g., web services]) from information system management (e.g., database management systems) functionality.

**Guidance**

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AS-2, DA-1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-2.1**

**Assessment Objective**

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.

## SC-3 – Security Function Isolation (High)

**Control**

The information system isolates security functions from nonsecurity functions.

**Guidance**

The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-3.1**

**Assessment Objective**

Determine if:
the organization defines the security functions of the information system to be isolated from non-security functions;

the information system isolates security functions from non-security functions.

**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; other relevant documents or records.

**Test:** Separation of security functions from non-security functions within the information system.

**SC-3(1) – Enhancement (High)**

**Control**

The information system implements underlying hardware separation mechanisms to facilitate security function isolation.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-3(1).1**

**Assessment Objective**

Determine if the information system implements underlying hardware separation mechanisms to facilitate security function isolation.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing security function isolation; information system design documentation; hardware separation mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Hardware separation mechanisms facilitating security function isolation.

| SC-3(2) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The information system isolates security functions enforcing access and information flow control from both nonsecurity functions and from other security functions. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-3(2).1** | | |
| **Assessment Objective**<br>Determine if the information system isolates security functions enforcing access and information flow control from both nonsecurity functions and other security functions.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Test:** Isolation of security functions enforcing access and information flow control. | | |
| **SC-3(3) – Enhancement (High)** | | |
| **Control**<br>The organization implements an information system isolation boundary to minimize the number of nonsecurity functions included within the boundary containing security functions. | | |
| **Guidance**<br>Nonsecurity functions contained within the isolation boundary are considered security-relevant. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-3(3).1** | | |
| **Assessment Objective**<br>Determine if the organization implements an information system isolation boundary to minimize the number of nonsecurity functions included within the boundary containing security functions. | | |

**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-3(4) – Enhancement (High)**

**Control**

The organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-3(4).1**

**Assessment Objective**

Determine if the organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.

**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-3(5) – Enhancement (High)**

**Control**

The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-3(5).1**

**Assessment Objective**

Determine if the organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

**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)**

**Control**

The information system prevents unauthorized and unintended information transfer via shared system resources.

**Implementation Standard(s)**

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.
2. (For FTI only) When authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

**Guidance**

The purpose of this control is to prevent sensitive information, including encrypted representations of sensitive information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remnence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the CMS information system for which there is only a single user/role.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; IRS-1075: 5.6.3.4#2, 5.6.3.4#3 | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: SC-4.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the information system prevents unauthorized and unintended information transfer via shared system resources.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.<br>**Examine:** Bulk record identities that have been transmitted externally.<br>**Test:** Information system for unauthorized and unintended transfer of information via shared system resources. | | |
| **SC-5 – Denial of Service Protection (High)** | | |
| **Control**<br>The information system protects against or limits the effects of the following types of denial of service attacks defined on the following sites or in the following documents:<br>- SANS Organization www.sans.org/dosstep;<br>- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and<br>- NIST CVE List http://checklists.nist.gov/home.cfm. | | |
| **Guidance**<br>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 devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: SC-5.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system;

the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.

**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)**

**Control**

The information system:
a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
b. Connects to external networks or information systems only through managed interfaces consisting of automated boundary protection devices arranged in accordance with an organizational security architecture.

**Implementation Standard(s)**

1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
2. Utilize stateful inspection/application firewall hardware and software.
3. Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

**Guidance**

Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected sub-network commonly referred to as a demilitarized zone or DMZ).

The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. When this situation occurs, the organization implements appropriate compensating security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AS-2 | **Related Controls**<br>**Requirement(s):** AC-4, CA-3, MP-4, RA-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7.1**

**Assessment Objective**

Determine if:

the organization defines the external boundary of the information system;

the organization defines key internal boundaries of the information system;

the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system;

the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

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 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; other relevant documents or records.

**Interview:** Selected organizational personnel with boundary protection responsibilities.

**Test:** Automated mechanisms implementing boundary protection capability within the information system.

## SC-7(1) – Enhancement (High)

**Control**

The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.

**Guidance**

Publicly accessible information system components include, for example, public web servers.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: SC-7(1).1

**Assessment Objective**

Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.

**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.

## SC-7(2) – Enhancement (High)

**Control**

The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(2).1**

**Assessment Objective**

Determine if:
the organization defines the mediation necessary for public access to the organization's internal networks;

the information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing access controls for public access to the organization's internal networks.

**SC-7(3) – Enhancement (High)**

**Control**

The organization limits the number of access points to the information system (e.g., prohibiting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

**Guidance**

Desktop modems allow backdoors into the network, putting the data and network at very high risk. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(3).1**

**Assessment Objective**

Determine if the organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

**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) – Enhancement (High)**

**Control**

The organization:
(a) Implements a managed interface for each external telecommunication service;
(b) Establishes a traffic flow policy for each managed interface;
(c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
(e) Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days; and
(f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

**Guidance**

"External telecommunication services" addresses transmissions of data to/from entities external to the secure site, including to other secure sites using networks or any other communication resources outside of the physical control of the secure site to transmit information.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(4).1**

**Assessment Objective**

Determine if:
the organization implements a managed interface for each external telecommunication service;

the organization establishes a traffic flow policy for each managed interface;

the organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;

the organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;

the organization reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days;

the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

**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; other relevant documents or records.

**Interview:** Selected organizational personnel with boundary protection responsibilities.

**Test:** Managed interfaces implementing organizational traffic flow policy.

**SC-7(5) – Enhancement (High)**

**Control**

The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(5).1**

**Assessment Objective**

Determine if:

the information system, at managed interfaces, denies network traffic by default;

the information system, at managed interfaces, allows network traffic by exception.

**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(6) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-7(6).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization prevents the unauthorized release of information outside of the information system boundary; or<br>the organization prevents any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.<br>**Test:** Automated mechanisms supporting the fail-safe boundary protection capability within the information system. | | |
| **SC-7(7) – Enhancement (High)** | | |
| **Control**<br>The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. | | |

**Guidance**

This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent split-tunneling. Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(7).1**

**Assessment Objective**

Determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

**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) – Enhancement (High)**

**Control**

The information system routes all internal communications traffic to external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.

**Guidance**

External networks are networks outside the control of the organization. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Proxy servers are also configurable with organization-defined lists of authorized and unauthorized websites.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(8).1**

**Assessment Objective**

Determine if:
the organization defines the internal communications traffic to be routed to external networks;

the organization defines the external networks to which the organization-defined internal communications traffic should be routed;

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.

**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-8 – Transmission Integrity (High)**

**Control**

The information system protects the integrity of transmitted information.

**Implementation Standard(s)**

1. Employ appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13).

**Guidance**

This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization implements appropriate compensating security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.312(c)(1) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-8.1**

**Assessment Objective**

Determine if:
the information system protects the integrity of transmitted information.

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 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-8(1) – Enhancement (High)**

**Control**

The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

**Guidance**

Alternative physical protection measures include, for example, protected distribution systems.

| **Applicability:** All | **Reference(s):** HIPAA: 164.312(c)(1) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-8(1).1**

**Assessment Objective**

Determine if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

**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-9 – Transmission Confidentiality (High)**

**Control**

The information system protects the confidentiality of transmitted information.

**Implementation Standard(s)**

1. (For PII only) When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

**Guidance**

This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization implements appropriate compensating security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, BP-2, BP-4; HIPAA: 164.312(e)(1); IRS-1075: 5.6.3.4#2, 5.6.3.4#4.1 | **Related Controls Requirement(s):** AC-17 |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-9.1**

**Assessment Objective**

Determine if:
the information system protects the confidentiality of transmitted information.

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 transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records.

**Examine:** Fax machine locations for secure custodial coverage of outgoing and incoming PII transmitted data.

**Test:** Transmission confidentiality capability within the information system.

**Test:** Send and/or receive a simulated PII fax.

**SC-9(1) – Enhancement (High)**

**Control**

The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

**Guidance**

Alternative physical protection measures include, for example, protected distribution systems.

| **Applicability:** All | **Reference(s):** HIPAA: 164.312(e)(1), 164.312(e)(2)(ii); IRS-1075: 5.6.3.4#2, 5.7#1 | **Related Controls Requirement(s):** SC-13 |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-9(1).1**

**Assessment Objective**

Determine if:
the organization optionally defines alternative physical measures to prevent unauthorized disclosure of information during transmission;

the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by organization-defined alternative physical measures.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Cryptographic mechanisms implementing transmission confidentiality capability within the information system.

| SC-10 – Network Disconnect (High) | | |
|---|---|---|
| **Control**<br>The information system automatically terminates the network connection associated with a communications session at the end of the session, or:<br>a. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and<br>b. Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity. | | |
| **Guidance**<br>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.<br>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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AS-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-10.1** | | |
| **Assessment Objective**<br>Determine if:<br>the information system automatically terminates a network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity; or<br>the information system:<br>- forcibly de-allocates communications session DHCP leases after seven (7) days; and<br>- forcibly disconnects inactive VPN connections after thirty (30) minutes of inactivity. | | |
| **Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.<br>**Test:** Network disconnect capability within the information system. | | |

| SC-12 – Cryptographic Key Establishment and Management (High) | | |
|---|---|---|
| **Control**<br>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. | | |
| **Guidance**<br>Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4; IRS-1075: 5.7.1#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-12.1** | | |
| **Assessment Objective**<br>Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.<br>**Assessment Methods And Objects**<br>**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.<br>**Interview:** Organizational personnel with responsibilities for cryptographic key establishment or management.<br>**Test:** Automated mechanisms implementing cryptographic key management and establishment within the information system. | | |
| **SC-12(1) – Enhancement (High)** | | |
| **Control**<br>The organization maintains availability of information in the event of the loss of cryptographic keys by users. Mechanisms are employed to: (i) prohibit the use of encryption keys that are not recoverable by authorized personnel, (ii) require senior management approval to authorize recovery of keys by other than the key owner, and (iii) comply with approved cryptography standards (see SC-13). | | |

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|
| **ASSESSMENT PROCEDURE: SC-12(1).1** | | |
| **Assessment Objective**<br>Determine if the organization maintains availability of information in the event of the loss of cryptographic keys by users.<br>**Assessment Methods And Objects**<br>**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 – Use of Cryptography (High)** | | |
| **Control**<br>When cryptographic mechanisms are used, the information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2, 5.6.3.4#4.2-3 | **Related Controls Requirement(s):** AC-3, SC-8.Std.1, SC-9(1) |
| **ASSESSMENT PROCEDURE: SC-13.1** | | |
| **Assessment Objective**<br>Determine if when cryptographic mechanisms are used, the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |

| SC-13(1) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-13(1).1** | | |
| **Assessment Objective**<br>Determine if when cryptographic mechanisms are used, the organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records. | | |
| **SC-14 – Public Access Protections (High)** | | |
| **Control**<br>The information system protects the integrity and availability of publicly available information and applications.<br>**Implementation Standard(s)**<br>1. Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.<br>2. If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix D: E-authentication Standard. | | |
| **Guidance**<br>The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.<br>CMS refers to the National Institute of Standards and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix D: E-authentication Standard provides a summary for remote access controls. | | |

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-14.1**

**Assessment Objective**

Determine if:
the information system protects the integrity and availability of publicly available information and applications.

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 public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms protecting the integrity and availability of publicly available information and applications within the information system.

**SC-15 – Collaborative Computing Devices (High)**

**Control**

The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall 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.

**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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-15.1**

**Assessment Objective**

Determine if:
the organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative;

if authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used;

if authorized, the information system prohibits remote activation of collaborative computing devices;

if authorized, the information system provides an explicit indication of use to users physically present at the devices.

**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) – Enhancement (High)**

**Control**

If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-15(1).1**

**Assessment Objective**

Determine if the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

**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:** Physical disconnect of collaborative computing devices.

## SC-17 – Public Key Infrastructure Certificates (High)

**Control**

The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

**Guidance**

This control focuses on certificates with a visibility external to the CMS information system and does not include certificates related to internal system operations, for example, application-specific time services. Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: SC-17.1

**Assessment Objective**

Determine if the organization issues public key certificates under the organization-defined certificate policy or obtains public key certificates under a certificate policy from an approved service provider.

**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)

**Control**

The organization:
a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

**Guidance**

Decisions regarding the employment of mobile code within CMS information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on CMS servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-18.1**

**Assessment Objective**

Determine if:
the organization defines acceptable and unacceptable mobile code and mobile code technologies;

the organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies;

the organization authorizes, monitors, and controls the use of mobile code within the information system.

**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)

**Control**

The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If authorized, the organization:
a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

| **Applicability:** All | **Reference(s):** FISCAM: CM-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-19.1**

**Assessment Objective**

Determine if:
the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously;

the organization authorizes, monitors, and controls the use of VoIP within the information system.

**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)**

**Control**

The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

**Guidance**

This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. 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. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: SC-20.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if the information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.<br>**Test:** Automated mechanisms implementing secure name/address resolution service (authoritative source). | | |
| **SC-20(1) – Enhancement (High)** | | |
| **Control**<br>The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains. | | |
| **Guidance**<br>An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-20(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces;<br>the information system, when operating as part of a distributed, hierarchical namespace, enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services). | | |

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**Test:** Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services.

**SC-21 – Secure Name /Address Resolution Service (Recursive or Caching Resolver) (High)**

**Control**

The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

**Guidance**

A recursive resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients. Authoritative DNS servers are examples of authoritative sources. 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-21.1**

**Assessment Objective**

Determine if the information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

**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) | | |
|---|---|---|
| **Control**<br>The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation. | | |
| **Guidance**<br>A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists). | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-22.1** | | |
| **Assessment Objective**<br>Determine if:<br>the information systems that collectively provide name/address resolution service for an organization are fault tolerant;<br>the information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.<br>**Assessment Methods And Objects**<br>**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.<br>**Test:** Automated mechanisms supporting name/address resolution service for fault tolerance and role separation. | | |

| SC-23 – Session Authenticity (High) | | |
|---|---|---|
| **Control**<br>The information system provides mechanisms to protect the authenticity of communications sessions. | | |
| **Guidance**<br>This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services). | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-23.1** | | |
| **Assessment Objective**<br>Determine if the information system provides mechanisms to protect the authenticity of communications sessions.<br>**Assessment Methods And Objects**<br>**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.<br>**Test:** Automated mechanisms implementing session authenticity. | | |
| **SC-24 – Fail in Known State (High)** | | |
| **Control**<br>The information system fails to a known secure state for all failures preserving the maximum amount of state information in failure. | | |

**Guidance**

Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps 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 the organization with less disruption of mission/business processes.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-24.1**

**Assessment Objective**

Determine if:
the organization defines the system state information that should be preserved in the event of a system failure;

the information system preserves organization-defined system state information in the event of a system failure.

**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)**

**Control**

The information system protects the confidentiality and integrity of information at rest.

**Guidance**

This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within a CMS information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-28.1**

**Assessment Objective**

Determine if the information system protects the confidentiality and integrity of information at rest.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records.

**Test:** Automated mechanisms implementing confidentiality and integrity protections for information at-rest.

## SC-32 – Information System Partitioning (High)

**Control**

The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

**Guidance**

Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-32.1**

**Assessment Objective**

Determine if the organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

**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)**

**Control**

Controls shall be implemented to protect CMS sensitive information that is sent via email.

**Implementation Standard(s)**

1. Prior to sending an email, place all CMS sensitive information in an encrypted attachment.

**Guidance**

A good place to obtain recommended security practices for handling sensitive information via e-mail is NIST SP 800-45 (as amended), Guidelines on Electronic Mail Security.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-CMS-1.1**

**Assessment Objective**

Determine if:
the organization effectively implements protections for CMS sensitive information that is sent via e-mail;
the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Email policy and procedures; other relevant documents or records.

**Interview:** Sample of organizational personnel who use email.

| SC-CMS-2 – Website Usage (High) | | |
|---|---|---|
| **Control**<br>CMS web sites are operated within the restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction. | | |
| **Guidance**<br>Monitor the CMS and DHHS security programs to determine is there are any modified directives and instruction. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-CMS-2.1** | | |
| **Assessment Objective**<br>Determine if the organization maintains CMS websites within restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction.<br>**Assessment Methods And Objects**<br>**Examine:** CMS web site baseline and change management documentation for appropriate configurations.<br>**Interview:** Web site administrators. | | |

# 17.0 SYSTEM AND INFORMATION INTEGRITY (SI) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **SI-1 – System and Information Integrity Policy and Procedures (High)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, BP-1, BP-2, BP-3, BP-4, CP-2, SM-1, SM-3; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system and information integrity policy; | | |

the organization system and information integrity policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities;

the organization develops and formally documents system and information integrity procedures;

the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls;

the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities.

the organization reviews/updates the system and information integrity policy and procedures within every three hundred sixty-five (365) days.

**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)**

**Control**

The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software updates related to flaw remediation for effectiveness and potential side effects on CMS information systems before installation; and
c. Incorporates flaw remediation into the organizational configuration management process.

**Implementation Standard(s)**

1. Correct identified information system flaws on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days.
(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.

**Guidance**

The organization identifies CMS information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) installs security-relevant software updates (e.g., patches, service packs, and hot fixes) within the CMS-designated time period. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in CMS information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts have been accomplished.

| **Applicability:** All | **Reference(s):** FISCAM: AS-3, CM-5; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls**<br>**Requirement(s):** CA-2, CA-4, CA-7, CM-3, IR-4, SI-11 |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-2.1**

**Assessment Objective**

Determine if:
the organization identifies, reports, and corrects information system flaws;

the organization tests software updates related to flaw remediation for effectiveness before installation;

the organization tests software updates related to flaw remediation for potential side effects on organizational information systems before installation;

the organization incorporates flaw remediation into the organizational configuration management process.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with flaw remediation responsibilities.

**SI-2(1) – Enhancement (High)**

**Control**

The organization centrally manages the flaw remediation process and installs software updates automatically.

**Guidance**

Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

| **Applicability:** All | **Reference(s):** HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-2(1).1**

**Assessment Objective**

Determine if:
the organization centrally manages the flaw remediation process;

the organization installs software updates automatically.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic 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; other relevant documents or records.

**Test:** Automated mechanisms supporting centralized management of flaw remediation and automatic software updates.

| SI-2(2) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation. | | |
| **Applicability:** All | **Reference(s):** HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-2(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation;<br>the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Test:** Automated mechanisms implementing information system flaw remediation update status. | | |

## SI-3 – Malicious Code Protection (High)

**Control**

The organization:
a. Employs malicious code protection mechanisms at CMS information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
- Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- Inserted through the exploitation of information system vulnerabilities;
b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with CMS configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
- Perform critical system file scans during system boot, information system scans using the frequency specified in Implementation Standard 1, 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 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 Standard(s)**

1. Desktop malicious code scanning software is configured to perform critical system file scans every twelve (12) hours.

**Guidance**

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong 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 CMS missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

| **Applicability:** All | **Reference(s):** FISCAM: CM-5; IRS-1075: 5.6.2.5#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-3.1**

**Assessment Objective**

Determine if:

the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code:

- transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- inserted through the exploitation of information system vulnerabilities;

the organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

- transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- inserted through the exploitation of information system vulnerabilities;

the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1;

the organization defines one or more of the following actions to be taken in response to malicious code detection:
- block malicious code;
- quarantine malicious code; and/or
- send alert to administrator;

the organization configures malicious code protection mechanisms to:
- perform periodic scans of the information system in accordance with organization-defined frequency;
- perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;
- take organization-defined action(s) in response to malicious code detection;

the organization addresses the receipt of false positives during malicious code:
- detection and eradication;
- the resulting potential impact on the availability of the information system.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with malicious code protection responsibilities.

**Test:** Automated mechanisms implementing malicious code protection capability.

## SI-3(1) – Enhancement (High)

**Control**

The organization centrally manages malicious code protection mechanisms.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.5#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: SI-3(1).1

**Assessment Objective**

Determine if the organization centrally manages malicious code protection mechanisms.

**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) – Enhancement (High)**

**Control**

The information system automatically updates malicious code protection mechanisms (including signature definitions).

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.5#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-3(2).1**

**Assessment Objective**

Determine if the information system automatically updates malicious code protection mechanisms, including signature definitions.

**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(3) – Enhancement (High)**

**Control**

The information system prevents non-privileged users from circumventing malicious code protection capabilities.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-3(3).1**

**Assessment Objective**

Determine if the information system prevents non-privileged users from circumventing malicious code protection capabilities.

**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.

**Test:** Automated mechanisms implementing malicious code protection capability.

## SI-4 – Information System Monitoring (High)

**Control**

The organization:
a. Monitors events on the information system in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks;
b. Identifies unauthorized use of the information system;
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and
e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

**Implementation Standard(s)**

1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.

**Guidance**

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). 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, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at 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. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, DA-1, SM-5; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4 | **Related Controls Requirement(s):** AC-8, AU-4, CM-6 |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4.1**

**Assessment Objective**

Determine if:

the organization monitors events on the information system in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks;

the organization identifies unauthorized use of the information system;

the organization deploys monitoring devices:
- strategically within the information system to collect organization-determined essential information;
- at ad hoc locations within the system to track specific types of transactions of interest to the organization;

the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with information system monitoring responsibilities.

**SI-4(1) – Enhancement (High)**

**Control**

The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4(1).1**

**Assessment Objective**

Determine if the organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

**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; other relevant documents or records.

**Test:** Information system-wide intrusion detection capability.

**SI-4(2) – Enhancement (High)**

**Control**

The organization employs automated tools to support near real-time analysis of events.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4(2).1**

**Assessment Objective**

Determine if the organization employs automated tools to support near real-time analysis of events.

**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; other relevant documents or records.

**Test:** Automated tools supporting near real-time event analysis.

**SI-4(3) – Enhancement (High)**

**Control**

The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4(3).1**

**Assessment Objective**

Determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

**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; other relevant documents or records.

**Test:** Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms.

| SI-4(4) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. | | |
| **Guidance**<br>Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-4(4).1** | | |
| **Assessment Objective**<br>Determine if:<br>the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.<br>the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. | | |
| **Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Test:** Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms. | | |

| SI-4(5) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The information system provides near real-time alerts when the following indications of compromise or potential compromise occur:<br>(a) Presence of malicious code,<br>(b) Unauthorized export of information,<br>(c) Signaling to an external information system, or<br>(d) Potential intrusions. | | |
| **Guidance**<br>Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-4(5).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines indicators of compromise or potential compromise to the security of the information system;<br>the information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs. | | |
| **Assessment Methods And Objects**<br>**Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.<br>**Test:** Information system monitoring real-time alert capability. | | |
| **SI-4(6) – Enhancement (High)** | | |
| **Control**<br>The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities. | | |

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4(6).1**

**Assessment Objective**

Determine if the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

**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; other relevant documents or records.

**Test:** Information system-wide intrusion detection and prevention capability.

**SI-5 – Security Alerts, Advisories, and Directives (High)**

**Control**

The organization:
a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to appropriate personnel; and
d. Implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.

**Guidance**

Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) 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 affects on CMS operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-3, CM-5, DA-1, SM-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-5.1**

**Assessment Objective**

Determine if:
the organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;

the organization generates internal security alerts, advisories, and directives;

the organization defines personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives;

the organization disseminates security alerts, advisories, and directives to organization-identified personnel;

the organization implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records.

**Interview:** Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system.

**SI-5(1) – Enhancement (High)**

**Control**

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-5(1).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

**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 Functionality Verification (High)

**Control**

The information system verifies the correct operation of system security functions upon system startup and restart, upon command by users with appropriate access, and on a monthly routine basis and to notify system administration when anomalies are discovered.

**Guidance**

The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization implements compensating security controls. Information system transitional states include, for example, startup, restart, shutdown, and abort.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, CM-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-6.1**

**Assessment Objective**

Determine if:

the organization defines the appropriate conditions, including the system transitional states if applicable, for verifying the correct operation of security functions;

the organization defines for periodic security function verification, the frequency of the verifications;

the organization defines information system responses and alternative action(s) to anomalies discovered during security function verification;

the information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification);

the information system responds to security function anomalies in accordance with organization-defined responses and alternative action(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-6(1) – Enhancement (High)**

**Control**

The information system provides notification of failed automated security tests.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-6(1).1**

**Assessment Objective**

Determine if the information system provides notification of failed automated security tests.

**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; automated security test results; other relevant documents or records.

**Test:** Automated mechanisms implementing alerts and/or notifications for failed automated security tests.

**SI-6(2) – Enhancement (High)**

**Control**

The information system provides automated support for the management of distributed security testing.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-6(2).1**

**Assessment Objective**

Determine if the information system provides automated support for the management of distributed security testing.

**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:** Automated mechanisms supporting the management of distributed security function testing.

**SI-7 – Software and Information Integrity (High)**

**Control**

The information system detects unauthorized changes to software and information.

**Guidance**

The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices consistent with CMS information security policy and procedures with regard to commercial-off-the-shelf (COTS) integrity mechanisms, and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications. Integrity mechanisms include, but are not limited to, parity checks, check-sums, error detection data validation techniques, cyclical redundancy checks, and cryptographic hashes to detect and protect against information tampering, errors, omissions and unauthorized changes to software.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, CM-4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-7.1**

**Assessment Objective**

Determine if the information system detects unauthorized changes to software and information.

**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) – Enhancement (High) | | |
|---|---|---|
| **Control**<br>The organization reassesses the integrity of software and information by performing daily integrity scans of the information system. | | |
| **Applicability:** All | **Reference(s):** HIPAA: 164.312(c)(2), 164.312(e)(2)(i) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-7(1).1** | | |
| **Assessment Objective**<br>Determine if the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.<br>**Assessment Methods And Objects**<br>**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) – Enhancement (High)** | | |
| **Control**<br>The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification. | | |
| **Applicability:** All | **Reference(s):** HIPAA: 164.312(c)(2), 164.312(e)(2)(i) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-7(2).1** | | |
| **Assessment Objective**<br>Determine if the organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification. | | |

**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-8 – Spam Protection (High)**

**Control**

The organization:
a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with CMS configuration management policy and procedures.

**Guidance**

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers.

| **Applicability:** All | **Reference(s):** FISCAM: CM-5; HIPAA: 164.308(a)(1)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-8.1**

**Assessment Objective**

Determine if:
the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means;

the organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means;

the organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1.

**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) – Enhancement (High)**

**Control**

The organization centrally manages spam protection mechanisms.

| **Applicability:** All | **Reference(s):** HIPAA: 164.308(a)(1)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-8(1).1**

**Assessment Objective**

Determine if the organization centrally manages spam protection mechanisms.

**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) – Enhancement (High)**

**Control**

The information system automatically updates spam protection mechanisms (including signature definitions).

| **Applicability:** All | **Reference(s):** HIPAA: 164.308(a)(1)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-8(2).1**

**Assessment Objective**

Determine if the information system automatically updates spam protection mechanisms (including signature definitions).

**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-9 – Information Input Restrictions (High)

**Control**

The organization restricts the capability to input information to the information system to authorized personnel.

**Guidance**

Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

| **Applicability:** All | **Reference(s):** FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.1 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: SI-9.1

**Assessment Objective**

Determine if the organization restricts the capability to input information to the information system to authorized personnel.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for implementing restrictions on individual authorizations to input information into the information system.

## SI-10 – Information Input Validation (High)

**Control**

The information system uses automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

**Guidance**

Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.

| **Applicability:** All | **Reference(s):** FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; IRS-1075: 5.6.2.5#1.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-10.1**

**Assessment Objective**

Determine if the information system uses automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

**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)**

**Control**

The information system:
a. Identifies potentially security-relevant error conditions;
b. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries; and
c. Reveals error messages only to authorized personnel.

**Guidance**

The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, User IDs, account numbers, social security numbers, and credit card numbers.

| **Applicability:** All | **Reference(s):** FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2 | **Related Controls Requirement(s):** SI-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-11.1**

**Assessment Objective**

Determine if:
the information system identifies potentially security-relevant error conditions;

the organization defines sensitive or potentially harmful information that should not be contained in error logs and administrative messages;

the information system generates error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries;

the information system reveals error messages only to authorized personnel.

**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 Output Handling and Retention (High)**

**Control**

The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**Implementation Standard(s)**

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 National Archives and Records Administration (NARA) requirements.

**Guidance**

The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention.

| **Applicability:** All | **Reference(s):** FISCAM: BP-2, BP-3; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-12.1**

**Assessment Objective**

Determine if:

the organization handles both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements;

the organization retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

the organization meets all the requirements specified in the applicable 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.

# CMS Information Security (IS)
# Acceptable Risk Safeguards (ARS)

## Appendix B - CMSR Moderate Impact Level Data

***(Rev.1, 05-24-11)***

## Table of Contents


1.0 Access Control (AC) – Technical 1

2.0 Awareness and Training (AT) – Operational 44

3.0 Audit and Accountability (AU) – *Technical* 51

4.0 Security Assessment and Authorization (CA) – *Management* 71

5.0 Configuration Management (CM) – *Operational* 87

6.0 Contingency Planning (CP) – *Operational* 107

7.0 Identification and Authentication (IA) – *Technical* 128

8.0 Incident Response (IR) – *Operational* 143

9.0 Maintenance (MA) – *Operational* 156

*10.0* Media Protection (MP) – *Operational* 168

11.0 Physical and Environmental Protection (PE) – *Operational* 184

12.0 Planning (PL) – *Management* 205

13.0 Personnel Security (PS) – *Operational* 213

14.0 Risk Assessment (RA) – *Management* 222

15.0 System and Services Acquisition (SA) – *Management* 230

16.0 System and Communications Protection (SC) – *Technical* 250

17.0 System and Information Integrity (SI) – *Operational* 279

# 1.0 ACCESS CONTROL (AC) – TECHNICAL

*(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)*

| AC-1 – Access Control Policy and Procedures (Moderate) | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AS-1, SM-1, SM-3; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents access control policy; | | |

the organization access control policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities;

the organization develops and formally documents access control procedures;

the organization access control procedures facilitate implementation of the access control policy and associated access controls;

the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities;

the organization reviews/updates the access control policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Access control policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with access control responsibilities.

| AC-2 – Account Management (Moderate) | | |
|---|---|---|
| **Control**<br>The organization manages information system accounts, including:<br>a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);<br>b. Establishing conditions for group membership;<br>c. Identifying authorized users of the information system and specifying access privileges;<br>d. Requiring appropriate approvals for requests to establish accounts;<br>e. Establishing, activating, modifying, disabling, and removing accounts;<br>f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;<br>g. Notifying account managers 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;<br>h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;<br>i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and<br>j. Reviewing accounts using the frequency specified in Implementation Standard 1.<br>**Implementation Standard(s)**<br>1. Review information system accounts within every one hundred eighty (180) days and require annual certification.<br>2. Remove or disable default user accounts. Rename active default accounts.<br>3. Implement centralized control of user access administrator functions.<br>4. Regulate the access provided to contractors and define security requirements for contractors. | | |
| **Guidance**<br>The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AC-4, AS-2, AS-4, BP-3, SD-2, SM-4; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AC-2.1**

**Assessment Objective**

Determine if:
the organization manages information system accounts, including;
- identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
- establishing conditions for group membership;
- identifying authorized users of the information system and specifying access privileges;
- requiring appropriate approvals for requests to establish accounts;
- establishing, activating, modifying, disabling, and removing accounts;
- specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- notifying account managers 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;
- deactivating: (a) temporary accounts that are no longer required; and (b) accounts of terminated or transferred users;
- granting access to the system based on: (a) a valid access authorization; (b) intended system usage; and (c) other attributes as required by the organization or associated missions/business functions;

the organization reviews information system accounts in accordance with the frequency specified in Implementation Standard 1.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing account management; security plan; list of active 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.

**Interview:** Organizational personnel with account management responsibilities.

**AC-2(1) – Enhancement (Moderate)**

**Control**

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

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#2.1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-2(1).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms to support information system account management functions.

**Assessment Methods And Objects**

**Examine:** Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**AC-2(2) – Enhancement (Moderate)**

**Control**

The information system automatically terminates emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three hundred sixty-five (365) days.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#2.1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-2(2).1**

**Assessment Objective**

Determine if:

the organization defines in the security plan, explicitly or by reference, a time period for each type of account after which the information system terminates temporary and emergency accounts;

the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.

**Assessment Methods And Objects**

**Examine:** Security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of active accounts; information system audit records; other relevant documents or records.

| AC-2(3) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The information system automatically disables inactive accounts after one hundred eighty (180) days. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#2.1 | **Related Controls**<br>**Requirement(s):** IA-4.Std.1 |
| **ASSESSMENT PROCEDURE: AC-2(3).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, a time period after which the information system disables inactive accounts;<br>the information system automatically disables inactive accounts after organization-defined time period.<br>**Assessment Methods And Objects**<br>**Examine:** Procedures addressing account management; 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; other relevant documents or records. | | |
| **AC-2(4) – Enhancement (Moderate)** | | |
| **Control**<br>The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#2.1 | **Related Controls**<br>**Requirement(s):** |

**ASSESSMENT PROCEDURE: AC-2(4).1**

**Assessment Objective**

Determine if:
the information system automatically audits:
- account creation;
- modification;
- disabling;
- termination actions;

the information system notifies, as required, appropriate individuals.

**Assessment Methods And Objects**

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

**AC-2(7) – Enhancement (Moderate)**

**Control**

The organization:
(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;
(b) Tracks and monitors privileged role assignments; and
(c) Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.

**Guidance**

Privileged roles include, for example, key management, network and system administration, database administration, web administration.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-2(7).1**

**Assessment Objective**

Determine if:
the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;

the organization tracks and monitors privileged role assignments;

the organization inspects administrator groups, root accounts and other system related accounts on demand, but at least once during the specified period to ensure that unauthorized accounts have not been created.

**Assessment Methods And Objects**

**Examine:** Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; information system audit records; audit tracking and monitoring reports; other relevant documents or records.

**Interview:** Organizational personnel with account management responsibilities.

**AC-3 – Access Enforcement (Moderate)**

**Control**

The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

**Implementation Standard(s)**

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).
2. If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix D: E-authentication Standard.
3. Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information.
4. Data stored in the information system must be protected with system access controls.

**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) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

Encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AS-1, AS-2, AS-3, AS-4, BP-2, BP-4, CM-3, DA-1, IN-2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3 | **Related Controls Requirement(s):** SC-13 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-3.1**

**Assessment Objective**

Determine if:

the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records.

| AC-3(1) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>[Withdrawn: Incorporated into AC-6]. | | |
| **AC-4 – Information Flow Enforcement (Moderate)** | | |
| **Control**<br>The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. | | |
| **Guidance**<br>Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) 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 content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-1, BP-2, BP-4, DA-1; IRS-1075: 5.6.3.2#2.2 | **Related Controls Requirement(s):** SC-7 |
| **ASSESSMENT PROCEDURE: AC-4.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines applicable policy for controlling the flow of information within the system and between interconnected systems;<br>the organization defines approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; | | |

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

**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.

**AC-5 – Separation of Duties (Moderate)**

**Control**

The organization:
a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
b. Documents separation of duties; and
c. Implements separation of duties through assigned information system access authorizations.

**Implementation Standard(s)**

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

**Guidance**

Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, AS-3, AS-4, BP-4, SD-1, SD-2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-5.1**

**Assessment Objective**

Determine if:
the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;

the organization documents separation of duties;

the organization implements separation of duties through assigned information system access authorizations.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties.

**AC-6 – Least Privilege (Moderate)**

**Control**

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

**Implementation Standard(s)**

1. Disable all file system access not explicitly required for system, application, and administrator functionality.
2. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.
3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.
4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.
5. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If authorized, boot access is password protected.

**Guidance**

The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to CMS operations and assets, individuals, other organizations, and the Nation.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AS-2, AS-3; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); HSPD 7: D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-6.1**

**Assessment Objective**

Determine if:
the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.

| AC-6(1) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization explicitly authorizes access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals. | | |
| **Guidance**<br>Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-6(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized;<br>the organization explicitly authorizes access to the organization-defined security functions and security-relevant information. | | |
| **Assessment Methods And Objects**<br>**Examine:** Access control policy; 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; other relevant documents or records.<br>**Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. | | |

| AC-6(2) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization requires that users of information system accounts, or roles, with access to administrator accounts or 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. | | |
| **Guidance**<br>This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy such as Role Based Access Control (RBAC) is being implemented 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. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-6(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access;<br>the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions;<br>the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions. | | |
| **Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.<br>**Interview:** Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. | | |

| AC-7 – Unsuccessful Login Attempts (Moderate) | | |
|---|---|---|
| **Control**<br>The information system:<br>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<br>b. Automatically disables or locks the account/node until released after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.<br>**Implementation Standard(s)**<br>1. Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user during a fifteen (15) minute time period. Require the lock out to persist for a minimum of one (1) hour. | | |
| **Guidance**<br>Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2; IRS-1075: 5.6.3.2#4.1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid login attempts occur;<br>the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period; | | |

the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:
- lock out the account/node for a specified time period;
- lock out the account/note until released by an administrator; or
- delay the next login prompt according to organization-defined delay algorithm;

the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded;

the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing unsuccessful login attempts; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

## AC-8 – System Use Notification (Moderate)

**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 for CMS information systems is:

- You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  * You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information 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 information system.
  * Any communication or data transiting or stored on this information 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: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

**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 CMS 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, web sites, web pages where substantial personal information from the public is collected, ftp, telnet, or other services accessed.

System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2 | **Related Controls Requirement(s):** SI-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-8.1**

**Assessment Objective**

Determine if:

the information system displays the CMS-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 and states that:

- users are accessing a U.S. Government information system;
- system usage may be monitored, recorded, and subject to audit;
- unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- use of the system indicates consent to monitoring and recording;

the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system;

the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; other relevant documents or records.

**ASSESSMENT PROCEDURE: AC-8.2**

**Assessment Objective**

Determine if:
the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access;

the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities;

the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.

**AC-10 – Concurrent Session Control (Moderate)**

**Control**

The information system limits the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.

**Guidance**

This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.
A session is 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-10.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the maximum number of concurrent sessions to be allowed for each system account;

the information system limits the number of concurrent sessions for each system account to the organization-defined number of sessions.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing concurrent session control; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records.

**AC-11 – Session Lock (Moderate)**

**Control**

The information system:
a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

**Guidance**

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AS-2; IRS-1075: 5.6.3.2#4.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-11.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the time period of user inactivity after which the information system initiates a session lock;

the information system initiates a session lock after the organization-defined time period of inactivity or upon receiving a request from a user;

the information system retains the session lock until the user reestablishes access using established identification and authentication procedures.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records.

**AC-12 – Session Termination (Moderate)**

**Control**

[Withdrawn: Incorporated into SC-10].

**AC-13 – Supervision and Review--Access Control (Moderate)**

**Control**

[Withdrawn: Incorporated into AC-2 and AU-6].

| AC-14 – Permitted Actions without Identification or Authentication (Moderate) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication; and<br>b. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.<br>**Implementation Standard(s)**<br>1. Identify and document specific user actions that can be performed on the information system without identification or authentication. | | |
| **Guidance**<br>This control is intended for public websites and other publicly available systems. It is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as http://www.usa.gov). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login 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 being repeated, but rather to situations where identification and/or authentication have not yet occurred. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AS-2 | **Related Controls Requirement(s):** IA-2 |
| **ASSESSMENT PROCEDURE: AC-14.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization identifies specific user actions that can be performed on the information system without identification or authentication; | | |

the organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

the organization meets all the requirements specified in the applicable 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; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records.

## AC-14(1) – Enhancement (Moderate)

**Control**

The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish CMS mission/business objectives.

| **Applicability:** All | **Reference(s):** HIPAA: 164.312(c)(1) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-14(1).1**

**Assessment Objective**

Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records.

## AC-15 – Automated Marking (Moderate)

**Control**

[Withdrawn: Incorporated into MP-3].

| AC-17 – Remote Access (Moderate) | | |
|---|---|---|
| **Control**<br>Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:<br>a. Documents allowed methods of remote access to the information system;<br>b. Establishes usage restrictions and implementation guidance for each allowed remote access method;<br>c. Monitors for unauthorized remote access to the information system;<br>d. Authorizes remote access to the information system prior to connection; and<br>e. Enforces requirements for remote connections to the information system.<br>**Implementation Standard(s)**<br>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.<br>2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix D: E-authentication Standard. | | |
| **Guidance**<br>This control requires explicit authorization prior to allowing remote access to a CMS information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to a CMS information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network (VPN) when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to CMS information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AC-4; IRS-1075: 5.6.3.2#5, 5.7.1#1 | **Related Controls Requirement(s):** IA-2, SC-9 |

**ASSESSMENT PROCEDURE: AC-17.1**

**Assessment Objective**

Determine if:
the organization documents allowed methods of remote access to the information system;
the organization establishes usage restrictions and implementation guidance for each allowed remote access method;
the organization monitors for unauthorized remote access to the information system;
the organization authorizes remote access to the information system prior to connection;
the organization enforces requirements for remote connections to the information system.
the organization meets all the requirements specified in the applicable 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; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with remote access authorization, monitoring, and control responsibilities.

**AC-17(1) – Enhancement (Moderate)**

**Control**

The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

**Guidance**

Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(1).1**

**Assessment Objective**

Determine if the information system employs automated mechanisms to facilitate the monitoring and control of remote access methods.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records.

**AC-17(2) – Enhancement (Moderate)**

**Control**

The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

**Guidance**

Use only the CMS-approved encryption standard (see SC-13).

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#5, 5.7.1#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(2).1**

**Assessment Objective**

Determine if the organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**AC-17(3) – Enhancement (Moderate)**

**Control**

The information system routes all remote accesses through a limited number of managed access control points.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(3).1**

**Assessment Objective**

Determine if:

the organization defines a limited number of managed access control points for remote access to the information system;

the information system routes all remote accesses through managed access control points.

**Assessment Methods And Objects**

**Examine:** Access control policy; 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; other relevant documents or records.

**AC-17(4) – Enhancement (Moderate)**

**Control**

The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.2#5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(4).1**

**Assessment Objective**

Determine if:
the organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs;

the organization documents the rationale for such access in the security plan for the information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records.

**AC-17(5) – Enhancement (Moderate)**

**Control**

The organization monitors for unauthorized remote connections to the information system at least quarterly, and takes appropriate action if an unauthorized connection is discovered.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(5).1**

**Assessment Objective**

Determine if:
the organization monitors for unauthorized remote connections to the information system in accordance with the organization-defined frequency;

the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered;

the organization takes organization-defined appropriate action(s) if an unauthorized connection is discovered.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for monitoring remote connections to the information system.

**AC-17(7) – Enhancement (Moderate)**

**Control**

The organization ensures that remote sessions used for remote administration employ additional security measures (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled) and the CMS-approved encryption standard (see SC-13), and the sessions are audited.

**Guidance**

Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(7).1**

**Assessment Objective**

Determine if:
the organization defines the security functions and security-relevant information that can be accessed using remote sessions;

the organization defines the additional security measures to be employed for remote sessions used to access organization-defined security functions and security-relevant information;

the organization employs the CMS-approved encryption standard (see SC-13) for remote sessions used to access organization-defined security functions and security-relevant information;

the organization audits remote sessions for accessing organization-defined security functions and security-relevant information, if required by the control.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records (if auditing is required); other relevant documents or records.

**AC-17(8) – Enhancement (Moderate)**

**Control**

The organization disables Bluetooth and peer-to-peer networking protocols within the information system except for explicitly identified components in support of specific operational requirements.

**Guidance**

The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17(8).1**

**Assessment Objective**

Determine if the organization disables Bluetooth and peer-to-peer networking protocols within the information system except for explicitly identified components in support of specific operational requirements.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; security plan; list of networking protocols deemed to be non-secure; other relevant documents or records.

## AC-18 – Wireless Access (Moderate)

**Control**

The organization prohibits the installation of wireless access points (WAP) to CMS information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If authorized, the organization:
a. Monitors for unauthorized wireless access to the information system; and
b. Enforces requirements for wireless connections to the information system.

**Implementation Standard(s)**

1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented:
(a) Encryption protection is enabled;
(b) Access points are placed in secure areas;
(c) Access points are shut down when not in use (i.e., nights, weekends);
(d) A firewall is implemented between the wireless network and the wired infrastructure;
(e) MAC address authentication is utilized;
(f) Static IP addresses, not DHCP, is utilized;
(g) Personal firewalls are utilized on all wireless clients;
(h) File sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall; and
(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

**Guidance**

Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AC-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-18.1**

**Assessment Objective**

Determine if:
the organization establishes usage restrictions and implementation guidance for wireless access;

the organization monitors for unauthorized wireless access to the information system;

the organization authorizes wireless access to the information system prior to connection;

the organization enforces requirements for wireless connections to the information system.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system.

**AC-18(1) – Enhancement (Moderate)**

**Control**

If wireless access is explicitly approved, the information system protects wireless access to the system using authentication and encryption.

**Guidance**

Authentication applies to user, device, or both as necessary.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-18(1).1**

**Assessment Objective**

Determine if the information system protects wireless access to the system using authentication and encryption.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

| AC-18(2) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points quarterly, and takes appropriate action if an unauthorized connection is discovered. | | |
| **Guidance**<br>Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-18(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, in accordance with organization-defined frequency;<br>the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered;<br>the organization takes appropriate action(s) if an unauthorized connection discovered. | | |
| **Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records.<br>**Interview:** Organizational personnel responsible for monitoring wireless connections to the information system. | | |

| AC-19 – Access Control for Mobile Devices (Moderate) |
| --- |
| **Control**<br>The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants [PDA], cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:<br>a. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;<br>b. Monitors for unauthorized connections of mobile devices to CMS information systems;<br>c. Enforces requirements for the connection of mobile devices to CMS information systems;<br>d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;<br>e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and<br>f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software. |

**Guidance**

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to 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). Examples of information system functionality that provide the capability for automatic execution of code are Auto-Run and Auto-Play. Organizational policies and procedures for mobile devices 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 measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures 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 family.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1; IRS-1075: 4.6#1 | **Related Controls Requirement(s):** MP-4, MP-5 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-19.1**

**Assessment Objective**

Determine if:

the organization prohibits the connection of portable and mobile devices to the information system unless explicitly authorized, in writing, by the CIO;

if authorized, the organization employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;

if authorized, the organization monitors for unauthorized connections of mobile devices to organizational information systems;

if authorized, the organization enforces requirements for the connection of mobile devices to organizational information systems;

if authorized, the organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

if authorized, the organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures;

if authorized, the organization defines the inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be of significant risk;

if authorized, the organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

**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; other relevant documents or records.

**Interview:** Organizational personnel who use portable and mobile devices to access the information system.

## AC-19(1) – Enhancement (Moderate)

**Control**

The organization restricts the use of writable, removable media in CMS information systems.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: AC-19(1).1

**Assessment Objective**

Determine if the organization restricts the use of writable, removable media in organizational information systems.

**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; other relevant documents or records.

**Interview:** Organizational personnel who use portable and mobile devices to access the information system.

| AC-19(2) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization prohibits the use of personally owned, removable media in CMS information systems. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-19(2).1** | | |
| **Assessment Objective**<br>Determine if the organization prohibits the use of personally owned, removable media in organizational information systems.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |
| **AC-19(3) – Enhancement (Moderate)** | | |
| **Control**<br>The organization prohibits the use of removable media in CMS information systems when the media has no identifiable owner. | | |
| **Guidance**<br>An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion). | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-19(3).1** | | |
| **Assessment Objective**<br>Determine if the organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner. | | |

**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; other relevant documents or records.

## AC-20 – Use of External Information Systems (Moderate)

**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 CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall 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 virtual private networking (VPN) and 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 Standard(s)**

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.
2. (For PII only) Only organization owned computers and software can be used to process, access, and store PII.

**Guidance**

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular 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. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies.

This control does not apply to the use of external information systems to access public interfaces to CMS information systems and information (e.g., individuals accessing federal information through www.medicare.gov). The organization establishes terms and conditions for the use of external information systems in accordance with CMS security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the CMS information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17.

| **Applicability:** All | **Reference(s):** FISCAM: SM-7; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-20.1**

**Assessment Objective**

Determine if:

the organization prohibits the use of external information systems to store, access, transmit, or process sensitive information unless explicitly authorized, in writing, by the CIO;

if authorized, the organization identifies individuals authorized to:
- access the information system from the external information systems;
- process, store, and/or transmit organization-controlled information using the external information systems;

if authorized, the terms and conditions address, at a minimum:
- the types of applications that can be accessed from external information systems;
- the maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
- how other users of the external information system will be prevented from accessing federal information;
- the use of virtual private networking (VPN) and firewall technologies;
- the use of and protection against the vulnerabilities of wireless technologies;
- the maintenance of adequate physical security controls;
- the use of virus and spyware protection software; and
- how often the security capabilities of installed software are to be updated.

the organization meets all the requirements specified in the applicable implementation standard(s).

only organizational owned computers and software are used to process, access, and store PII.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems.

**AC-20(1) – Enhancement (Moderate)**

**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) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

| | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** IRS-1075: 4.7.2#1 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AC-20(1).1**

**Assessment Objective**

Determine if 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:
- can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
- has approved information system connection or processing agreements with the organizational entity hosting the external information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing the use of external information systems; security plan; information system connection or processing agreements; account management documents; other relevant documents or records.

**AC-20(2) – Enhancement (Moderate)**

**Control**

The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

**Guidance**

Limits on the use of organization-controlled portable storage media in external information systems can 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.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-20(2).1**

**Assessment Objective**

Determine if the organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing the use of external information systems; security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records.

## AC-22 – Publicly Accessible Content (Moderate)

**Control**

The organization:
a. Designates individuals authorized to post information onto a CMS information system that is publicly accessible;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the CMS information system;
d. Reviews the content on the publicly accessible CMS information system for nonpublic information monthly; and
e. Removes nonpublic information from the publicly accessible CMS information system, if discovered.

**Guidance**

Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on a CMS information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-CMS information systems is covered by appropriate organizational policy.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-22.1**

**Assessment Objective**

Determine if:
the organization designates individuals authorized to post information onto a CMS information system that is publicly accessible;

the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the CMS information system;

the organization reviews the content on the publicly accessible CMS information system for nonpublic information monthly;

the organization removes nonpublic information from the publicly accessible CMS information system, if discovered.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records; other relevant documents or records.

**Interview:** Organizational personnel responsible for managing publicly accessible information posted on organizational information systems.

# 2.0AWARENESS AND TRAINING (AT) – OPERATIONAL

*(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)*

| AT-1 – Security Awareness and Training Policy and Procedures (Moderate) | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular CMS information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SM-1, SM-3, SM-7; IRS-1075: 5.6.2.7#1.1-2, 6.1#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AT-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security awareness and training policy; | | |

the organization security awareness and training policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities, and compliance;

the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities;

the organization develops and formally documents security awareness and training procedures;

the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls;

the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities;

the organization reviews/updates the security awareness and training policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with security awareness and training responsibilities.

**AT-2 – Security Awareness (Moderate)**

**Control**

The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by system changes, and within every three hundred sixty-five (365) days thereafter.

**Guidance**

The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the CMS information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to CMS' information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SM-4; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AT-2.1**

**Assessment Objective**

Determine if:

the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually;

the organization provides refresher security awareness training in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records.

**Interview:** Organizational personnel comprising the general information system user community.

**AT-3 – Security Training (Moderate)**

**Control**

The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) refresher training within every three hundred sixty-five (365) days thereafter.

**Implementation Standard(s)**

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 system changes; and refresher training within every three hundred sixty-five (365) days thereafter.

**Guidance**

The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of CMS and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of CMS' information security program.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-4; IRS-1075: 5.6.2.7#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AT-3.1**

**Assessment Objective**

Determine if:
the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes;

the organization provides role-based security-related refresher training within every three hundred sixty-five (365) days thereafter.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for role-based, security-related training; organizational personnel with significant information system security responsibilities.

| AT-4 – Security Training Records (Moderate) |
| --- |
| **Control**<br>The organization:<br>a. Documents and monitors individual CMS information system security training activities including basic security awareness training and specific information system security training; and<br>b. Retains individual training records for three (3) years. |

**Guidance**

Procedures and training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
1) All users of CMS information systems must be exposed to security awareness materials at least annually. 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 basics and policy level training in security planning and management.
3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) 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.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-4; IRS-1075: 6.2#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AT-4.1**

**Assessment Objective**

Determine if:
the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training;

the organization retains individual training records in accordance with the organization-defined time period.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.

**Interview:** Organizational personnel with security training record retention responsibilities.

# 3.0AUDIT AND ACCOUNTABILITY (AU) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **AU-1 – Audit and Accountability Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular CMS information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, SM-1, SM-3; IRS-1075: 5.6.3.3#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents audit and accountability policy; | | |

the organization audit and accountability policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities;

the organization develops and formally documents audit and accountability procedures;

the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls;

the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities.

the organization reviews/updates the audit and accountability policy and procedures within every three hundred sixty-five (365) days.

**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 – Auditable Events (Moderate)

**Control**

The organization:
a. Determines, based on a risk assessment and CMS mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
c. Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

**Implementation Standard(s)**

1. Generate audit records for the following events:
(a) User account management activities,
(b) System shutdown,
(c) System reboot,
(d) System errors,
(e) Application shutdown,
(f) Application restart,
(g) Application errors,
(h) File creation,
(i) File deletion,
(j) File modification,
(k) Failed and successful log-ons,
(l) Security policy modifications, and
(m) Use of administrator privileges.
2. Enable logging for perimeter devices, including firewalls and routers.
(a) Log packet screening denials originating from un-trusted networks,
(b) Packet screening denials originating from trusted networks,
(c) User account management,
(d) Modification of packet filters,
(e) Application errors,
(f) System shutdown and reboot,
(g) System errors, and
(h) Modification of proxy services.
3. Verify that proper logging is enabled in order to audit administrator activities.
4. (For FTI only) Generate audit records for the following events in addition to those specified in other controls:
(a) All successful and unsuccessful authorization attempts.
(b) All changes to logical access control authorities (e.g., rights, permissions).
(c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
(d) The audit trail shall capture the enabling or disabling of audit report generation services.
(e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

**Guidance**

The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system 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 extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AC-5, AS-2, DA-1; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1 | **Related Controls Requirement(s):** AU-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-2.1**

**Assessment Objective**

Determine if:

the organization determines, based on a risk assessment and CMS mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;

the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events;

the organization provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;

the organization defines in the security plan, explicitly or by reference, information system auditable events;

the organization defines the subset of auditable events defined in (a) that are to be audited within the information system and (b) the frequency of (or situation requiring) auditing for each identified event;

the organization determines, based on current threat information and ongoing assessment of risk, the subset of auditable events defined in (a) to be audited within the information system, and (b) the frequency of (or situation requiring) auditing for each identified event.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records.

**Interview:** Organizational personnel with auditing and accountability responsibilities.

**AU-2(1) – Enhancement (Moderate)**

**Control**

[Withdrawn: Incorporated into AU-12].

**AU-2(2) – Enhancement (Moderate)**

**Control**

[Withdrawn: Incorporated into AU-12].

**AU-2(3) – Enhancement (Moderate)**

**Control**

The organization reviews and updates the list of auditable events within every three hundred sixty-five (365) days.

**Guidance**

The list of auditable events is defined in AU-2.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.3.3#2.1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-2(3).1**

**Assessment Objective**

Determine if the organization reviews and updates the list of organization-defined auditable events in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing auditable events; security plan; list of organization-defined auditable events; auditable events review and update records; information system audit records; information system incident reports; other relevant documents or records.

**Interview:** Organizational personnel with auditing and accountability responsibilities.

| AU-2(4) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization includes execution of privileged functions in the list of events to be audited by the information system, including administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-2(4).1** | | |
| **Assessment Objective**<br>Determine if the organization includes execution of privileged functions in the list of events to be audited by the information system.<br>**Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing auditable events; information system configuration settings and associated documentation; list of organization-defined auditable events; list of privileged security functions; other relevant documents or records. | | |
| **AU-3 – Content of Audit Records (Moderate)** | | |
| **Control**<br>The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.<br>**Implementation Standard(s)**<br>1. (For PHI only) 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. | | |
| **Guidance**<br>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. | | |

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-2, DA-1; IRS-1075: 5.6.3.3#3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-3.1**

**Assessment Objective**

Determine if:
the information system produces audit records that contain sufficient information to, at a minimum, establish:
- what type of event occurred;
- when (date and time) the event occurred;
- where the event occurred;
- the source of the event;
- the outcome (success or failure) of the event;
- the identity of any user/subject associated with the event.

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; other relevant documents or records.

**AU-3(1) – Enhancement (Moderate)**

**Control**

The information system includes the capability to include more detailed information in the audit records for audit events identified by type, location, or subject.

**Guidance**

An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: AU-3(1).1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization defines the additional, more detailed information to be included in audit records for audit events identified by type, location, or subject;<br>the information system includes the organization-defined additional, more detailed information in the audit records for audit events identified by type, location, or subject.<br>**Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records. | | |
| **AU-4 – Audit Storage Capacity (Moderate)** | | |
| **Control**<br>The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. | | |
| **Guidance**<br>The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.3.3#4 | **Related Controls Requirement(s):** AU-2, AU-5, AU-6, AU-7, SI-4 |
| **ASSESSMENT PROCEDURE: AU-4.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization allocates audit record storage capacity;<br>the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded. | | |

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**AU-5 – Response to Audit Processing Failures (Moderate)**

**Control**

The information system:
a. Alerts designated organizational officials in the event of an audit processing failure; and
b. Takes the following additional actions in response to an audit failure or audit storage capacity issue:
- Shutdown the information system,
- Stop generating audit records, or
- Overwrite the oldest records, in the case that storage media is unavailable.

**Guidance**

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, DA-1 | **Related Controls Requirement(s):** AU-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-5.1**

**Assessment Objective**

Determine if:
the organization defines designated organizational officials to be alerted in the event of an audit processing failure;
the organization defines in the security plan, explicitly or by reference, personnel to be notified in case of an audit processing failure;
the organization defines additional actions to be taken in the event of an audit processing failure;
the information system takes the additional organization-defined actions in the event of an audit processing failure.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

**AU-6 – Audit Review, Analysis, and Reporting (Moderate)**

**Control**

The organization:
a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

**Implementation Standard(s)**

1. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment.
2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment.
3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
4. Use automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior.
5. Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.
6. Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.
7. (For FTI only) All requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log. (see IRS Pub. 1075, sect 6.3.1)

**Guidance**

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to CMS operations, CMS assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AC-5, AS-2, DA-1, SM-5; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1 | **Related Controls Requirement(s):** AU-4, IR-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-6.1**

**Assessment Objective**

Determine if:
the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency;

the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

the organization report findings of inappropriate/unusual activities, to designated organizational officials.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** Logs for requests of FTI include receipt and/or disposal or FTI information is returned.

**Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities.

**Interview:** Organizational personnel responsible for handling FTI.

**ASSESSMENT PROCEDURE: AU-6.2**

**Assessment Objective**

Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit review, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities.

## AU-6(1) – Enhancement (Moderate)

**Control**

The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

| **Applicability:** All | **Reference(s):** HIPAA: 164.312(b) | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: AU-6(1).1

**Assessment Objective**

Determine if the information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities.

## AU-6(2) – Enhancement (Moderate)

**Control**

[Withdrawn: Incorporated into SI-4].

## AU-7 – Audit Reduction and Report Generation (Moderate)

**Control**

The information system provides an audit reduction and report generation capability.

**Guidance**

An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** AU-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-7.1**

**Assessment Objective**

Determine if the information system provides an audit reduction and report generation capability.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system audit review, analysis, and reporting responsibilities.

**AU-7(1) – Enhancement (Moderate)**

**Control**

The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-7(1).1**

**Assessment Objective**

Determine if the information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

**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; other relevant documents or records.

**AU-8 – Time Stamps (Moderate)**

**Control**

The information system uses internal system clocks to generate time stamps for audit records.

**Guidance**

Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-8.1**

**Assessment Objective**

Determine if the information system uses internal system clocks to generate time stamps for audit records.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**AU-8(1) – Enhancement (Moderate)**

**Control**

The information system synchronizes internal information system clocks daily and at system boot.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: AU-8(1).1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, the frequency of internal clock synchronization for the information system;<br>the organization defines the authoritative time source for internal clock synchronization;<br>the organization synchronizes internal information system clocks with the organization-defined authoritative time source in accordance with the organization-defined frequency.<br>**Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing time stamp generation; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. | | |
| **AU-9 – Protection of Audit Information (Moderate)** | | |
| **Control**<br>The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | | |
| **Guidance**<br>Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-9.1** | | |
| **Assessment Objective**<br>Determine if the information system protects audit information and audit tools from unauthorized:<br>- access;<br>- modification;<br>- deletion. | | |

**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; other relevant documents or records.

## AU-10 – Non-Repudiation (Moderate)

**Control**

The information system protects against an individual falsely denying having performed a particular action.

**Guidance**

Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. 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. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-10.1**

**Assessment Objective**

Determine if the information system protects against an individual falsely denying having performed a particular action.

**Assessment Methods And Objects**

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

| AU-11 – Audit Record Retention (Moderate) | | |
|---|---|---|
| **Control**<br>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.<br>**Implementation Standard(s)**<br>1. (For FTI only) Employ a permanent system of standardized records of request for disclosure of FTI and maintain the records for five (5) years or the applicable records control schedule, whichever is longer.<br>2. (For FTI only) To support the audit of FTI activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored.<br>3. (For PII only) Audit inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed. | | |
| **Guidance**<br>The organization retains 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. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-11.1** | | |
| **Assessment Objective**<br>Determine if:<br>the retention period for audit records is consistent with the records retention policy;<br>the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. | | |

the organization employs mechanisms to facilitate the review of PII disclosures/access records and retains the records for five (5) years or the applicable records control schedule, whichever is longer;

the organization ensures that audit information is archived for six (6) years to enable the recreation of computer related accesses to both the operation system and the application wherever PII is stored;

the organizational PII inspection reports include a record of corrective actions, which is retained for a minimum of three (3) years from the date the inspection was completed.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

**Examine:** PII disclosure/access audit records; PII audit information; PII inspection records; other relevant documents or records.

**Interview:** Organizational personnel with information system audit record retention responsibilities.

## AU-12 – Audit Generation (Moderate)

**Control**

The information system:
a. Provides audit record generation capability for the following events in addition to those specified in other controls:
- 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 shall capture the enabling or disabling of audit report generation services.
- The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).
b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and
c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

**Guidance**

Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-12.1**

**Assessment Objective**

Determine if:
the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2;

the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2;

the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system;

the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system audit record generation responsibilities.

**AU-12(1) – Enhancement (Moderate)**

**Control**

The information system compiles audit records from multiple components throughout the system into a system-wide (logical or physical) time-correlated audit trail.

**Guidance**

The audit trail is 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.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-12(1).1**

**Assessment Objective**

Determine if:

the information system produces a system-wide (logical or physical) audit trail of information system audit records;

the organization defines the information system components from which audit records are to be compiled into the system-wide audit trail;

the information system compiles audit records from organization-defined information system components into the system-wide audit trail;

the organization defines the acceptable level of tolerance for relationship between time stamps of individual records in the system-wide audit trail;

the system-wide audit trail is time-correlated to within the organization-defined level of tolerance to achieve a time ordering of audit records.

**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; other relevant documents or records.

# 4.0SECURITY ASSESSMENT AND AUTHORIZATION (CA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CA-1 – Security Assessment and Authorization Policies and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security assessment and authorization family [formerly called Certification and Accreditation [C&A] family and process). The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 5.6.1.4#1.1-2 | **Related Controls**<br>**Requirement(s):** CA-6 |
| **ASSESSMENT PROCEDURE: CA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security assessment and authorization policy; | | |

the organization security assessment and authorization policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities;

the organization develops and formally documents security assessment and authorization procedures;

the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls;

the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities;

the organization reviews/updates the security assessment and authorization policies and procedures within every three hundred sixty-five (365) days;

**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 (Moderate)

**Control**

The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system 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 the security requirements for the system;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

**Implementation Standard(s)**

1. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems.
2. The annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period.
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, ISSO).

**Guidance**

The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by CMS, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the FISMA annual assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring. The organization establishes 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 provided that the results are current, valid, and relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-3, SM-5; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1 | **Related Controls Requirement(s):** CA-4, CA-6, CA-7, CA-7(1), CA-7(2), SA-11, SI-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-2.1**

**Assessment Objective**

Determine if:
the organization develops a security assessment plan for the information system;

the security assessment plan describes the scope of the assessment including:
- security controls and control enhancements under assessment;
- assessment procedures to be used to determine security control effectiveness;
- assessment environment, assessment team, and assessment roles and responsibilities.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Security assessment policy; procedures addressing security assessments; security plan; security assessment plan; assessment evidence; other relevant documents or records.

**ASSESSMENT PROCEDURE: CA-2.2**

**Assessment Objective**

Determine if:
the organization assesses the security controls in the information system within every three hundred sixty-five (365) days in accordance with the CMS IS ARS Including 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 the security requirements for the system;

the organization provides the results of the security control assessment within every 365 days, in writing, to the Business Owner;

the Business Owner reviews the assessment documentation and updates system security documentation where necessary to reflect any changes to the system;

the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records.

**Interview:** Organizational personnel with security assessment responsibilities.

**CA-2(1) – Enhancement (Moderate)**

**Control**

The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

**Guidance**

An independent assessor or assessment team is any individual or group capable of conducting an impartial assessment of a CMS information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, accuracy, integrity, and reliability of the results.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-2(1).1**

**Assessment Objective**

Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

**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); other relevant documents or records.

**Interview:** Organizational personnel with security assessment responsibilities.

| CA-3 – Information System Connections (Moderate) |
|---|
| **Control**<br>The organization:<br>a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;<br>b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and<br>c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.<br>**Implementation Standard(s)**<br>1. Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location. |
| **Guidance**<br>This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between CMS and a nonfederal (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, SM-1; HSPD 7: F(19) | **Related Controls Requirement(s):** SA-9, SC-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-3.1**

**Assessment Objective**

Determine if:
the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);

the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;

the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated;

the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.

the organization meets all the requirements specified in the applicable 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; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records.

**Interview:** Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements.

**CA-4 – Security Certification (Moderate)**

**Control**

[Withdrawn: Incorporated into CA-2].

## CA-5 – Plan of Action and Milestones (POA&M) (Moderate)

**Control**

The organization:
a. Develops and submits a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

**Guidance**

The POA&M is a key document in the security authorization package and is subject to federal reporting requirements established by OMB.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-5, SM-6; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4 | **Related Controls Requirement(s):** CA-7 |
|---|---|---|

### ASSESSMENT PROCEDURE: CA-5.1

**Assessment Objective**

Determine if:
the organization develops a plan of action and milestones for the information system within thirty (30) days of the final results for every internal/external audit/review or test;

the plan of action and milestones documents 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;

the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates;

the organization updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.

**Interview:** Organizational personnel with plan of action and milestones development and implementation responsibilities.

**CA-5(1) – Enhancement (Moderate)**

**Control**

The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-5(1).1**

**Assessment Objective**

Determine if the organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is:
- accurate;
- up to date;
- readily available.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; plan of action and milestones; other relevant documents or records.

**Interview:** Organizational personnel with plan of action and milestones development and implementation responsibilities.

| CA-6 – Security Authorization (Moderate) |
|---|
| **Control**<br>The organization updates the security authorization:<br>- At least every three (3) years;<br>- When substantial changes are made to the system;<br>- When changes in requirements result in the need to process data of a higher sensitivity;<br>- When changes occur to authorizing legislation or federal requirements;<br>- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and<br>- Prior to expiration of a previous security authorization. |
| **Guidance**<br>Security authorization is the official management decision, conveyed through the authorization decision document, given by the CMS CIO or his/her designated representative (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to CMS operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of 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.<br>Through the security authorization process, the CMS CIO is accountable for the security risks associated with CMS information system operations. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the CMS CIO and the applicable information system Business Owner with an up-to-date status of the security state of the information system.<br>To reduce the administrative cost of security reauthorization, the CMS CIO uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. OMB policy requires that federal information systems are reauthorized at least every three years or when there is a significant change to the system.<br>A significant change to the information system includes a physical, administrative, or technical modification that alters the degree of protection required. Examples include, but are not limited to, changes in operating systems, computer hardware, firmware, operational environment, or system boundaries; new services or applications; or other conditions that potentially impact the system's security posture or authorization status. |

| **Applicability:** All | **Reference(s):** FISCAM: SM-2, SM-5; HSPD 7: F(19) | **Related Controls**<br>**Requirement(s):** CA-1, CA-2, CA-4, CA-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-6.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the frequency of authorization updates, not to exceed three years;

the organization updates the security authorization:
- at least every three (3) years;
- when substantial 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;
- 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;

a senior organizational official signs and approves the security authorization package.

**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); other relevant documents or records.

**Interview:** Organizational personnel with security authorization responsibilities.

| CA-7 – Continuous Monitoring (Moderate) | | |
|---|---|---|
| **Control**<br>The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:<br>a. A configuration management process for the information system and its constituent components;<br>b. A determination of the security impact of changes to the information system and environment of operation;<br>c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and<br>d. Reporting the security state of the information system to appropriate organizational officials within every three hundred sixty-five (365) days. | | |
| **Guidance**<br>A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-5; HSPD 7: F(19) | **Related Controls**<br>**Requirement(s):** CA-2, CA-4, CA-5, CA-6, CM-4, SI-2 |
| **ASSESSMENT PROCEDURE: CA-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization establishes a continuous monitoring strategy and program;<br>the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials;<br>the organization defines organizational officials to whom the security state of the information system should be reported; | | |

the organization implements a continuous monitoring program that includes:
- a configuration management process for the information system and its constituent components;
- a determination of the security impact of changes to the information system and environment of operation;
- ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records.

**Interview:** Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities.

## CA-7(1) – Enhancement (Moderate)

**Control**

The use of independent security assessment agents or teams to monitor security controls is not required. However, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.

**Guidance**

The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's three-year authorization cycle. See supplemental guidance for CA-2, enhancement (1), for further information on assessor independence.

| **Applicability:** All | **Reference(s):** HSPD 7: F(19) | **Related Controls**<br>**Requirement(s):** AC-9, CA-2 |
|---|---|---|

### ASSESSMENT PROCEDURE: CA-7(1).1

**Assessment Objective**

Determine if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

**Interview:** Organizational personnel with continuous monitoring responsibilities.

## CA-7(2) – Enhancement (Moderate)

**Control**

CMS plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all CMS information systems and information systems that are processing data on behalf of or directly for CMS including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures.

**Guidance**

Examples of vulnerability mitigation procedures are contained in Information Assurance Vulnerability Alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing could also provide evidence of independent validation. See supplemental guidance for CA-2, enhancement (2) for further information on malicious user testing, penetration testing, and other forms of security testing.

| **Applicability:** All | **Reference(s):** | **Related Controls**<br>**Requirement(s):** CA-2 |
|---|---|---|

### ASSESSMENT PROCEDURE: CA-7(2).1

**Assessment Objective**

Determine if:
the organization defines:
- the forms of security testing to be included in planning, scheduling, and security control assessments selecting from in-depth monitoring, malicious user testing, penetration testing, or an organization-defined form of security testing to ensure compliance with all vulnerability mitigation procedures;
- the frequency for conducting each form of security testing;
- whether the security testing will be announced or unannounced;

the organization plans, schedules, and conducts assessments using organization-defined forms of security testing in accordance with the organization-defined frequency and assessment techniques established for each form of testing to ensure compliance with all vulnerability mitigation procedures.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing vulnerability mitigation; 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.

# 5.0CONFIGURATION MANAGEMENT (CM) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CM-1 – Configuration Management Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-1, CP-2, SM-1, SM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents configuration management policy; | | |

the organization configuration management policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities;

the organization develops and formally documents configuration management procedures;

the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls;

the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities;

the organization reviews/updates the configuration management policy and procedures within every three hundred sixty-five (365) days.

**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 (Moderate)**

**Control**

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

**Guidance**

This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of a CMS information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with CMS' enterprise architecture.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2.1**

**Assessment Objective**

Determine if:
the organization develops and documents a baseline configuration of the information system;
the organization maintains, under configuration control, a current baseline configuration of the information system.
the organization documents deviations from the baseline configuration, in support of mission needs/objectives.

**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; other relevant documents or records.

**CM-2(1) – Enhancement (Moderate)**

**Control**

The organization reviews and updates the baseline configuration of the information system:
(a) At least once every three hundred sixty-five (365) days;
(b) When required due to major system changes/upgrades; and
(c) As an integral part of information system component installations and upgrades.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2(1).1**

**Assessment Objective**

Determine if:
the organization defines:
- the frequency of reviews and updates to the baseline configuration of the information system;
- the circumstances that require reviews and updates to the baseline configuration of the information system;

the organization reviews and updates the baseline configuration of the information system:
- in accordance with the organization-defined frequency;
- when required due to organization-defined circumstances;
- as an integral part of information system component installations and upgrades.

**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; other relevant documents or records.

**Interview:** Organizational personnel with configuration change control responsibilities.

**CM-2(3) – Enhancement (Moderate)**

**Control**

The organization retains older versions of baseline configurations as deemed necessary to support rollback.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-2(3).1**

**Assessment Objective**

Determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback.

**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; other relevant documents or records.

| CM-2(4) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization:<br>(a) Develops and maintains a list of software programs authorized (white list) or unauthorized (black list) to execute on the information system; and<br>(b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-2(4).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and maintains a list of software programs not authorized to execute on the information system;<br>the organization employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.<br>**Assessment Methods And Objects**<br>**Examine:** Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software programs not authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records. | | |

| CM-3 – Configuration Change Control (Moderate) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Determines the types of changes to the information system that are configuration controlled;<br>b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;<br>c. Documents approved configuration-controlled changes to the system;<br>d. Retains and reviews records of configuration-controlled changes to the system;<br>e. Audits activities associated with configuration-controlled changes to the system; and<br>f. 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 which meets 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. | | |
| **Guidance**<br>The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-3, BP-2, CM-3, CM-5, CM-6, CP-2; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** CM-4, CM-6, SI-2 |
| **ASSESSMENT PROCEDURE: CM-3.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization determines the types of changes to the information system that are configuration controlled;<br>the organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses; | | |

the organization documents approved configuration-controlled changes to the system;

the organization retains and reviews records of configuration-controlled changes to the system;

the organization audits activities associated with configuration-controlled changes to the system;

the organization defines:
- the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities;
- the frequency with which the configuration change control element convenes, and/or;
- configuration change conditions that prompt the configuration change control element to convene;

the organization 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 which meets 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.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with configuration change control responsibilities.

**CM-3(2) – Enhancement (Moderate)**

**Control**

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

**Guidance**

The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the CMS information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-3(2).1**

**Assessment Objective**

Determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

**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; other relevant documents or records.

**Interview:** Organizational personnel with configuration change control responsibilities.

**CM-4 – Security Impact Analysis (Moderate)**

**Control**

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.

**Guidance**

Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system.

| **Applicability:** All | **Reference(s):** FISCAM: AS-3, CM-3, CM-4, SM-5 | **Related Controls Requirement(s):** CA-7, CM-3 |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-4.1**

**Assessment Objective**

Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

**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 architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.

**CM-4(1) – Enhancement (Moderate)**

**Control**

The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-4(1).1**

**Assessment Objective**

Determine if:
the organization analyzes new software in a separate test environment before installation in an operational environment;

the organization, when analyzing new software in a separate test environment, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

**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; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.

**CM-4(2) – Enhancement (Moderate)**

**Control**

The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

**Guidance**

Changes include information system upgrades and modifications.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-4(2).1**

**Assessment Objective**

Determine if the organization, after the information system is changed, checks the security functions to verify that the functions are:
- implemented correctly;
- operating as intended;
- producing the desired outcome with regard to meeting the security requirements for the system.

**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; 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 (Moderate)**

**Control**

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.

**Guidance**

Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of 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 are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AS-3, CM-3, CM-4; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-5.1**

**Assessment Objective**

Determine if:

the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

the organization generates, reviews, and retains records reflecting all such changes.

**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; other relevant documents or records.

**Interview:** Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities.

## CM-6 – Configuration Settings (Moderate)

**Control**

The organization:
a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

**Implementation Standard(s)**

1. 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 all security configuration guidelines is as follows:
(a) CMS
(b) DHHS
(c) OMB
(d) NIST
(e) DISA.

**Guidance**

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AS-3, CM-2, CM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** CM-3, CM-8, SI-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-6.1**

**Assessment Objective**

Determine if:

the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed;

the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;

the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;

the organization implements the security configuration settings;

the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements;

the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with security configuration responsibilities.

**CM-6(3) – Enhancement (Moderate)**

**Control**

The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-6(3).1**

**Assessment Objective**

Determine if:

the organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability;

the organization ensures that such detected events are tracked, monitored, corrected, and available for historical purposes.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; procedures addressing incident response planning; information system design documentation; information system configuration settings and associated documentation; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities.

| CM-7 – Least Functionality (Moderate) | | |
|---|---|---|
| **Control**<br>The organization configures the information system to provide only essential capabilities and specifically disables, prohibits, or restricts the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled. | | |
| **Guidance**<br>Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential CMS operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, 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 server or web server, not both). The functions and services provided by CMS information systems, or individual components of CMS information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components 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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-3, CM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines for the information system prohibited or restricted:<br>- functions;<br>- ports;<br>- protocols;<br>- services; | | |

the organization configures the information system to provide only essential capabilities;

the organization configures the information system to specifically prohibit or restrict the use of organization-defined:
- functions;
- ports;
- protocols; and/or
- services.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.

**CM-7(1) – Enhancement (Moderate)**

**Control**

The organization reviews the information system within every three hundred sixty-five (365) days to identify and eliminate unnecessary functions, ports, protocols, and/or services.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-7(1).1**

**Assessment Objective**

Determine if:
the organization defines the frequency of information system reviews to identify and eliminate unnecessary:
- functions;
- ports;
- protocols; and/or
- services;

the organization reviews the information system in accordance with organization defined frequency to identify and eliminate unnecessary:
- functions;
- ports;
- protocols; and/or
- services.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the information system

## CM-8 – Information System Component Inventory (Moderate)

**Control**

The organization develops, documents, and maintains an inventory of information system components that:
a. Accurately reflects the current information system;
b. Is consistent with the authorization boundary of the information system;
c. Is at the level of granularity deemed necessary for tracking and reporting;
d. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and
e. Is available for review and audit by designated organizational officials.

**Guidance**

Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, 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.

| **Applicability:** All | **Reference(s):** FISCAM: CM-2, SM-1; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii) | **Related Controls Requirement(s):** CM-6 |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-8.1**

**Assessment Objective**

Determine if:
the organization defines information deemed necessary to achieve effective property accountability;

the organization develops, documents, and maintains an inventory of information system components that:
- accurately reflects the current information system;
- is consistent with the authorization boundary of the information system;
- is at the level of granularity deemed necessary for tracking and reporting;
- includes organization-defined information deemed necessary to achieve effective property accountability;
- is available for review and audit by designated organizational officials.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; other relevant documents or records.

**CM-8(1) – Enhancement (Moderate)**

**Control**

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

| **Applicability:** All | **Reference(s):** HIPAA: 164.310(d)(1), 164.310(d)(2)(iii) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-8(1).1**

**Assessment Objective**

Determine if the organization updates the inventory of information system components as an integral part of component:
- installations;
- removals;
- information system updates.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records.

**Interview:** Organizational personnel with information system installation and inventory responsibilities.

| CM-8(5) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-8(5).1** | | |
| **Assessment Objective**<br>Determine if the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.<br>**Assessment Methods And Objects**<br>**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; component installation records; other relevant documents or records.<br>**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 (Moderate)** | | |
| **Control**<br>The organization develops, documents, and implements a configuration management plan for the information system that:<br>a. Addresses roles, responsibilities, and configuration management processes and procedures;<br>b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and<br>c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items. | | |

**Guidance**

Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-9.1**

**Assessment Objective**

Determine if the organization develops, documents, and implements a configuration management plan for the information system that:
- addresses roles, responsibilities, and configuration management processes and procedures;
- defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management;
- establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing configuration management planning; security plan; other relevant documents or records.

# 6.0CONTINGENCY PLANNING (CP) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CP-1 – Contingency Planning Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-5, CP-1, CP-3, SM-1, SM-3; HIPAA: 164.308(a)(7)(i), 164.308(a)(7)(ii)(B); IRS-1075: 5.6.2.2#1.1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents contingency planning policy; | | |

the organization contingency planning policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities;

the organization develops and formally documents contingency planning procedures;

the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls;

the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities;

the organization reviews/updates the contingency planning policy and procedures within every three hundred sixty-five (365) days.

**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 (Moderate) |
|---|
| **Control**<br>The organization:<br>a. Develops a Contingency Plan (CP) for the information system that:<br>- Identifies essential CMS missions and business functions and associated contingency requirements;<br>- Provides recovery objectives, restoration priorities, and metrics;<br>- Addresses contingency roles, responsibilities, assigned individuals with contact information;<br>- Addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure;<br>- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and<br>- Is reviewed and approved by designated officials within the organization;<br>b. Distributes copies of the CP plan to key contingency personnel (identified by name and/or by role) and organizational elements;<br>c. Coordinates contingency planning activities with incident handling activities;<br>d. Reviews the CP for the information system within every three hundred sixty-five (365) days;<br>e. Revises the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing; and<br>f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements. |
| **Guidance**<br>Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for CMS mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Copies of the current CP are stored in a secure location at an alternate site accessible by management and other key personnel. |

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-1, CP-2, CP-3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-2.1**

**Assessment Objective**

Determine if:
the organization develops a contingency plan for the information system that:
- identifies essential missions and business functions and associated contingency requirements;
- provides recovery objectives, restoration priorities, and metrics;
- addresses contingency roles, responsibilities, assigned individuals with contact information;
- addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;
-is reviewed and approved by designated officials within the organization;

the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan;

the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities.

**ASSESSMENT PROCEDURE: CP-2.2**

**Assessment Objective**

Determine if:
the organization coordinates contingency planning activities with incident handling activities;

the organization defines the frequency of contingency plan reviews;

the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;

the organization revises 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;

the organization communicates contingency plan changes to the key contingency personnel and organizational elements.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities.

**CP-2(1) – Enhancement (Moderate)**

**Control**

The organization coordinates contingency plan development with organizational elements responsible for related plans.

**Guidance**

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Critical Infrastructure Plan, and Incident Response Plan.

| **Applicability:** All | **Reference(s):** HIPAA: 164.308(a)(7)(ii)(E); HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-2(1).1**

**Assessment Objective**

Determine if the organization coordinates the contingency plan development with other organizational elements responsible for related plans.

**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) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. | | |
| **Applicability:** All | **Reference(s):** HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-2(2).1** | | |
| **Assessment Objective**<br>Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records.<br>**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities. | | |
| **CP-3 – Contingency Training (Moderate)** | | |
| **Control**<br>The organization trains operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days. | | |
| **Guidance**<br>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 confirmed that appropriate training has been completed. | | |
| **Applicability:** All | **Reference(s):** FISCAM: CP-2; HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |

| ASSESSMENT PROCEDURE: CP-3.1 | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system;<br>the organization defines in the security plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is at least annually;<br>the organization provides refresher training in accordance with organization-defined frequency.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records.<br>**Interview:** Organizational personnel with contingency planning, plan implementation, and training responsibilities. | | |
| **CP-4 – Contingency Plan Testing and Exercises (Moderate)** | | |
| **Control**<br>The organization:<br>a. Tests and/or exercises the contingency plan for the CMS information system within every three hundred sixty-five (365) days using defined tests and exercises, such as the tabletop test in accordance with the current CMS contingency plan procedure to determine the plan's effectiveness and the organization's readiness to execute the plan; and<br>b. Documents and reviews the contingency plan test/exercise results and initiates reasonable and appropriate corrective actions to close or reduce the impact of contingency plan failures and deficiencies. | | |
| **Guidance**<br>There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on CMS operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-2, CP-4; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: CP-4.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted;

the organization defines in the security plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is at least annually;

the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;

the organization reviews the contingency plan test/exercise results and takes corrective actions.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises.

**CP-4(1) – Enhancement (Moderate)**

**Control**

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

**Guidance**

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Critical Infrastructure Plan, and Incident Response Plan.

| **Applicability:** All | **Reference(s):** HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-4(1).1**

**Assessment Objective**

Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.

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

**CP-5 – Contingency Plan Update (Moderate)**

**Control**

[Withdrawn: Incorporated into CP-2].

**CP-6 – Alternate Storage Site (Moderate)**

**Control**

The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.

**Guidance**

The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with CMS' recovery time objectives and recovery point objectives.

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-2, CP-3; IRS-1075: 5.6.2.2#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-6.1**

**Assessment Objective**

Determine if:
the organization establishes an alternate storage site;

the organization initiates necessary alternate storage site agreements to permit the storage and recovery of information system backup information.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records.

| CP-6(1) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. | | |
| **Guidance**<br>Hazards of concern to the organization are typically defined in an organizational assessment of risk. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.4 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-6(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the contingency plan identifies the primary storage site hazards;<br>the alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.<br>**Assessment Methods And Objects**<br>**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records. | | |
| **CP-6(3) – Enhancement (Moderate)** | | |
| **Control**<br>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. | | |
| **Guidance**<br>Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.4 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: CP-6(3).1**

**Assessment Objective**

Determine if:
the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster;

the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.

**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; other relevant documents or records.

**CP-7 – Alternate Processing Site (Moderate)**

**Control**

The organization:
a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; and
b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the time period for resumption specified in Implementation Standard 1.

**Implementation Standard(s)**

1. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within one (1) week of contingency plan activation.

**Guidance**

Equipment and supplies required to resume operations within the CMS-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with CMS recovery time objectives.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, CP-3; IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-7.1**

**Assessment Objective**

Determine if:
the organization establishes an alternate processing site;

the organization includes necessary alternate processing site agreements to permit the resumption of information system operations within the time period specified in Implementation Standard 1;

the equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the time period for resumption specified in Implementation Standard 1.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; security plan; spare equipment and supplies at alternate processing site; equipment and supply contracts; service level agreements; other relevant documents or records.

**CP-7(1) – Enhancement (Moderate)**

**Control**

The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.

**Guidance**

Hazards that might affect the information system are typically defined in the risk assessment.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-7(1).1**

**Assessment Objective**

Determine if:
the contingency plan identifies the primary processing site hazards;

the alternate processing site is separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

**CP-7(2) – Enhancement (Moderate)**

**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.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-7(2).1**

**Assessment Objective**

Determine if:
the organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster;

the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

**CP-7(3) – Enhancement (Moderate)**

**Control**

the organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-7(3).1**

**Assessment Objective**

Determine if alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records.

**CP-7(5) – Enhancement (Moderate)**

**Control**

The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-7(5).1**

**Assessment Objective**

Determine if the alternate processing site provides information security measures equivalent to that of the primary site.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

**CP-8 – Telecommunications Services (Moderate)**

**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 period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable.

**Implementation Standard(s)**

1. 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.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, CP-3; IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-8.1**

**Assessment Objective**

Determine if:
the organization establishes alternate telecommunications services to support the information system;

the organization establishes necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for CMS missions and business functions within the time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; list of essential missions and business functions; other relevant documents or records.

**CP-8(1) – Enhancement (Moderate)**

**Control**

The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-8(1).1**

**Assessment Objective**

Determine if:
the organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements;

the organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

**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; other relevant documents or records.

**CP-8(2) – Enhancement (Moderate)**

**Control**

The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-8(2).1**

**Assessment Objective**

Determine if the organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

**Interview:** Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.

**CP-9 – Information System Backup (Moderate)**

**Control**

The organization:
a. Conducts backups of user-level information contained in the CMS information system in accordance with the frequency specified in Implementation Standard 1;
b. Conducts backups of system-level information contained in the CMS information system in accordance with the frequency specified in Implementation Standard 1;
c. Conducts backups of CMS information system documentation including security-related documentation and other forms of data, including paper records; and
d. Protects the confidentiality and integrity of CMS backup information at the storage location.

**Implementation Standard(s)**

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.
2. (For PII only) Ensure that a current, retrievable, copy of PII is available before movement of servers.

**Guidance**

System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control.
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.

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-2; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6 | **Related Controls Requirement(s):** MP-4, MP-5 |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-9.1**

**Assessment Objective**

Determine if:
the organization backs up user-level information in accordance with the frequency specified in Implementation Standard 1;

the organization backs up system-level information in accordance with the frequency specified in Implementation Standard 1;

the organization backs up information system documentation (including security-related information and other forms of data).

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; backup storage location(s); information system backup logs or records; other relevant documents or records.

**Interview:** Organizational personnel with information system backup responsibilities.

**ASSESSMENT PROCEDURE: CP-9.2**

**Assessment Objective**

Determine if the organization protects the confidentiality and integrity of backup information at the storage location.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; information system configuration settings and associated documentation; backup storage location(s); other relevant documents or records.

**Interview:** Organizational personnel with information system backup responsibilities.

**CP-9(1) – Enhancement (Moderate)**

**Control**

The organization tests backup information following each backup to verify media reliability and information integrity.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.2#1.6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-9(1).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the frequency of information system backup testing;

the organization conducts information system backup testing in accordance with organization-defined frequency to verify backup media reliability and information integrity.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; information system backup test results; backup storage location(s); other relevant documents or records.

| CP-9(4) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>[Withdrawn: Incorporated into CP-9]. | | |
| **CP-10 – Information System Recovery and Reconstitution (Moderate)** | | |
| **Control**<br>The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.<br>**Implementation Standard(s)**<br>1. Secure information system recovery and reconstitution includes, but not limited to:<br>(a) Reset all system parameters (either default or organization-established),<br>(b) Reinstall patches,<br>(c) Reestablish configuration settings,<br>(d) Reinstall application and system software, and<br>(e) Fully test the system. | | |
| **Guidance**<br>Recovery is executing information system contingency plan activities to restore essential CMS missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on CMS priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. | | |
| **Applicability:** All | **Reference(s):** FISCAM: CP-2, CP-3, CP-4; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: CP-10.1**

**Assessment Objective**

Determine if:
the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure;

the organization provides for the recovery of the information system after a failure or other contingency in a trusted, secure, and verifiable manner.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**CP-10(1) – Enhancement (Moderate)**

**Control**

[Withdrawn: Incorporated into CP-4].

**CP-10(2) – Enhancement (Moderate)**

**Control**

The information system implements transaction recovery for systems that are transaction-based.

**Guidance**

Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-10(2).1**

**Assessment Objective**

Determine if the information system implements transaction recovery for systems that are transaction-based.

**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; other relevant documents or records.

**CP-10(3) – Enhancement (Moderate)**

**Control**

The organization provides compensating security controls for circumstances that inhibit recovery and reconstitution to a known state.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-10(3).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state;

the organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan test procedures; security plan; other relevant documents or records.

**Interview:** Organizational personnel with information system recovery and reconstitution responsibilities.

# 7.0IDENTIFICATION AND AUTHENTICATION (IA) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **IA-1 – Identification and Authentication Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.3.1#1.1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents identification and authentication policy; | | |

the organization identification and authentication policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities;

the organization develops and formally documents identification and authentication procedures;

the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls;

the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities;

the organization reviews/updates the identification and authentication policy and procedures within every three hundred sixty-five (365) days.

**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) (Moderate)**

**Control**

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

**Implementation Standard(s)**

1. Require the use of system and/or network authenticators and unique user identifiers.
2. Help desk support requires user identification for any transaction that has information security implications.

**Guidance**

Organizational users (i.e., CMS information system users) include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to CMS information systems is defined as either local or network. Local access is any access to a CMS information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to a CMS information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.

The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 5.6.3.1#1.2, 5.6.3.3#2.3 | **Related Controls Requirement(s):** AC-14, AC-17, MA-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2.1**

**Assessment Objective**

Determine if:

the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**IA-2(1) – Enhancement (Moderate)**

**Control**

The information system uses multifactor authentication for network access to privileged accounts.

| **Applicability:** All | **Reference(s):** HIPAA: 164.312(d); IRS-1075: 5.6.3.1#1.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(1).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for network access to privileged accounts.

**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; other relevant documents or records.

**IA-2(2) – Enhancement (Moderate)**

**Control**

The information system uses multifactor authentication for network access to non-privileged accounts.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(2).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for network access to non-privileged accounts.

**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; other relevant documents or records.

**IA-2(3) – Enhancement (Moderate)**

**Control**

The information system uses multifactor authentication for local access to privileged accounts.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(3).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for local access to privileged accounts.

**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; other relevant documents or records.

**IA-2(8) – Enhancement (Moderate)**

**Control**

The information system uses replay resistant authentication mechanisms for network access to privileged accounts.

**Guidance**

An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(8).1**

**Assessment Objective**

Determine if:
the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts;

the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.

**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; other relevant documents or records.

**IA-3 – Device Identification and Authentication (Moderate)**

**Control**

The information system uniquely identifies and authenticates specific and/or types of devices before establishing a connection.

**Guidance**

The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AC-2; IRS-1075: 5.6.3.1#1.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-3.1**

**Assessment Objective**

Determine if:
the organization defines the specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system;

the information system uniquely identifies and authenticates the organization-defined devices before establishing a connection to the information system.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.

**IA-4 – Identifier Management (Moderate)**

**Control**

The organization manages CMS information system identifiers for users and devices by:
a. Receiving authorization from a designated organizational official to assign a user or device identifier;
b. Selecting an identifier that uniquely identifies an individual or device;
c. Assigning the user identifier to the intended party or the device identifier to the intended device;
d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired; and
e. Disabling the user identifier after the time period of inactivity specified in Implementation Standard 1 and deleting disabled accounts during the annual re-certification process.

**Implementation Standard(s)**

1. Disable user identifiers after one hundred eighty (180) days of inactivity.

**Guidance**

Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system).

Reviews and validation of system users' accounts are conducted to ensure the continued need for access to a system. Identifier management is applicable to shared information system accounts (i.e., guest and anonymous).

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AC-4, AS-2; IRS-1075: 5.6.3.1#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-4.1**

**Assessment Objective**

Determine if:

the organization manages information system identifiers for users and devices by:

- receiving authorization from a designated organizational official to assign a user or device identifier;
- selecting an identifier that uniquely identifies an individual or device;
- assigning the user identifier to the intended party or the device identifier to the intended device;
- preventing reuse of user or device identifiers for the organization-defined time period;
- disabling the user identifier after the organization-defined time period of inactivity;

the organization defines in the security plan, explicitly or by reference, the time period of inactivity after which a user identifier is to be disabled.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records.

**Interview:** Organizational personnel with identifier management responsibilities.

| IA-5 – Authenticator Management (Moderate) |
|---|
| **Control**<br>The organization manages CMS information system authenticators for users and devices by:<br>a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;<br>b. Establishing initial authenticator content for authenticators defined by the organization;<br>c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;<br>d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;<br>e. Changing default content of authenticators upon information system installation;<br>f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);<br>g. Changing/refreshing password authenticators as defined in IA-5(1);<br>h. Protecting authenticator content from unauthorized disclosure and modification; and<br>i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. |
| **Guidance**<br>User 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). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The CMS information system supports user authenticator management by security 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 verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost 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. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2; IRS-1075: 5.6.3.1#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-5.1**

**Assessment Objective**

Determine if:
the organization defines the time period (by authenticator type) for changing/refreshing authenticators;

the organization manages information system authenticators for users and devices by:
- verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- establishing initial authenticator content for authenticators defined by the organization;
- ensuring that authenticators have sufficient strength of mechanism for their intended use;
- establishing and implementing administrative procedures for initial authenticator distribution;
- establishing and implementing administrative procedures for lost/compromised or damaged authenticators;
- establishing and implementing administrative procedures for revoking authenticators;
- changing default content of authenticators upon information system installation;
- establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);
- changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;
- protecting authenticator content from unauthorized disclosure and modification;
- requiring users to take, and having devices implement, specific measures to safeguard authenticators.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for determining initial authenticator content.

| IA-5(1) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The CMS information system, for password-based authentication:<br>(a) Automatically forces users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days;<br>(b) Prohibits the use of dictionary names or words;<br>(c) Enforces minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lower-case letters, and numbers) and/or special characters;<br>(d) Enforces at least a minimum of four (4) changed characters when new passwords are created;<br>(e) Encrypts passwords in storage and in transmission;<br>(f) Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum; and<br>(g) Prohibits password reuse for six (6) generations prior to reuse. | | |
| **Guidance**<br>This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does not apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-5(1).1** | | |
| **Assessment Objective**<br>Determine if the information system, for password-based authentication:<br>- enforces the minimum password complexity standards that meet the organization-defined requirements;<br>- enforces the organization-defined minimum number of characters that must be changed when new passwords are created;<br>- encrypts passwords in storage and in transmission;<br>- enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters;<br>- prohibits password reuse for the organization-defined number of generations. | | |

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**IA-5(2) – Enhancement (Moderate)**

**Control**

The CMS information system, for PKI-based authentication:
(a) Validates certificates by constructing a certification path with status information to an accepted trust anchor;
(b) Enforces authorized access to the corresponding private key; and
(c) Maps the authenticated identity to the user account.

**Guidance**

Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-5(2).1**

**Assessment Objective**

Determine if the information system, for PKI-based authentication:
- validates certificates by constructing a certification path with status information to an accepted trust anchor;
- enforces authorized access to the corresponding private key;
- maps the authenticated identity to the user account.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for PKI-based authentication management.

| IA-5(3) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization requires that the registration process to receive hardware tokens be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-5(3).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official;<br>the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).<br>**Assessment Methods And Objects**<br>**Examine:** Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; other relevant documents or records.<br>**Interview:** Organizational personnel with authenticator management responsibilities. | | |
| **IA-6 – Authenticator Feedback (Moderate)** | | |
| **Control**<br>The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. | | |
| **Guidance**<br>The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2; IRS-1075: 5.6.3.1#1.2 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: IA-6.1**

**Assessment Objective**

Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**IA-7 – Cryptographic Module Authentication (Moderate)**

**Control**

The information system uses 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-7.1**

**Assessment Objective**

Determine if the information system uses 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.

**Assessment Methods And Objects**

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

**IA-8 – Identification and Authentication (Non-Organizational Users) (Moderate)**

**Control**

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

**Guidance**

Non-organizational users include all CMS information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with 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). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered 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 to CMS operations, CMS assets, individuals, other organizations, and the Nation. Identification and authentication requirements for CMS information system access by organizational users are described in IA-2. If E-Authentication is used, refer to ARS Appendix D: E-authentication Standard.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-8.1**

**Assessment Objective**

Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

**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; other relevant documents or records.

# 8.0INCIDENT RESPONSE (IR) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **IR-1 – Incident Response Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-1, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents incident response policy; | | |

the organization incident response policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities;

the organization develops and formally documents incident response procedures;

the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls;

the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities;

the organization reviews/updates the incident response policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Incident response policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with incident response responsibilities.

**IR-2 – Incident Response Training (Moderate)**

**Control**

The organization:
a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and
b. Provides refresher training within every three hundred sixty-five (365) days.

**Guidance**

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Incident response training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. 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 basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
(4) CIOs, IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.2.6#2.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-2.1**

**Assessment Objective**

Determine if:
the organization identifies personnel with incident response roles and responsibilities with respect to the information system;

the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;

incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually;

the organization provides refresher incident response training in accordance with organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records.

**Interview:** Organizational personnel with incident response training and operational responsibilities.

**IR-3 – Incident Response Testing and Exercises (Moderate)**

**Control**

The organization tests and/or exercises the incident response capability for the information system within every three hundred sixty-five (365) days using reviews, analyses, and simulations to determine the incident response effectiveness and documents the results.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.2.6#2.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-3.1**

**Assessment Objective**

Determine if:
the organization defines incident response tests/exercises;

the organization defines in the security plan, explicitly or by reference, the frequency of incident response tests/exercises and the frequency is at least annually;

the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;

the organization documents the results of incident response tests/exercises;

the organization determines the effectiveness of the incident response capability.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing material; incident response test results; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with incident response testing responsibilities.

**IR-4 – Incident Handling (Moderate)**

**Control**

The organization:
a. Implements an incident handling capability using CMS Information Security Incident Handling and Breach Notification Procedures;
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 Standard(s)**

1. Document relevant information related to a security incident according to CMS Information Security Incident Handling and Breach Notification Procedures.
2. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.
3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure.

**Guidance**

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3 | **Related Controls Requirement(s):** AU-6, PE-6, SI-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-4.1**

**Assessment Objective**

Determine if:
the organization implements an incident handling capability for security incidents that includes:
- preparation;
- detection and analysis;
- containment;
- eradication;
- recovery;

the organization coordinates incident handling activities with contingency planning activities;

the organization incorporates lessons learned from ongoing incident handling activities into:
- incident response procedures;
- training;
- testing/exercises;

the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.

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; other relevant documents or records.

**Interview:** Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities.

**IR-4(1) – Enhancement (Moderate)**

**Control**

The organization employs automated mechanisms to support the incident handling process.

**Guidance**

An online incident management system is an example of an automated mechanism.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-4(1).1**

**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; other relevant documents or records.

**Interview:** Organizational personnel with incident handling responsibilities.

**IR-5 – Incident Monitoring (Moderate)**

**Control**

The organization tracks and documents information system security incidents.

**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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, SM-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#2.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-5.1**

**Assessment Objective**

Determine if the organization tracks and documents information system security incidents.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with incident monitoring responsibilities.

**IR-6 – Incident Reporting (Moderate)**

**Control**

The organization:
a. Requires personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current CMS Information Security Incident Handling and Breach Analysis/Notification Procedure; and
b. Reports security incident information to designated authorities.

**Guidance**

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. CMS requires that events and confirmed security incidents must be reported to the CMS IT Service Desk in accordance with established procedures.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-6.1**

**Assessment Objective**

Determine if:
the organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current CMS Information Security Incident Handling and Breach Analysis/Notification Procedure;

the organization reports security incident information to designated authorities.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with incident reporting responsibilities.

| IR-6(1) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms to assist in the reporting of security incidents. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-6(1).1** | | |
| **Assessment Objective**<br>Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.<br>**Assessment Methods And Objects**<br>**Examine:** Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; incident response plan; other relevant documents or records.<br>**Interview:** Organizational personnel with incident reporting responsibilities. | | |
| **IR-7 – Incident Response Assistance (Moderate)** | | |
| **Control**<br>The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents. | | |
| **Guidance**<br>Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. The CMS IT Service Desk is available to offer advice to users of a CMS information system. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>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; | | |

the incident response support resource is an integral part of the organization's incident response capability.

**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.

**IR-7(1) – Enhancement (Moderate)**

**Control**

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

**Guidance**

Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-7(1).1**

**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 assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records.

**Interview:** Organizational personnel with incident response support and assistance responsibilities; organizational personnel that require incident response support and assistance.

| IR-8 – Incident Response Plan (Moderate) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Develops an incident response plan that:<br>- Provides the organization with a roadmap for implementing its incident response capability;<br>- Describes the structure and organization of the incident response capability;<br>- Provides a high-level approach for how the incident response capability fits into the overall organization;<br>- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;<br>- Defines reportable incidents;<br>- Provides metrics for measuring the incident response capability within the organization.<br>- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and<br>- Is reviewed and approved by designated officials within the organization;<br>b. Distributes copies of the incident response plan to incident response personnel and organizational elements;<br>c. Reviews the incident response plan within every three hundred sixty-five (365) days;<br>d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and<br>e. Communicates incident response plan changes to incident response personnel and organizational elements. | | |
| **Guidance**<br>It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: IR-8.1**

**Assessment Objective**

Determine if the organization develops an incident response plan that:
- provides the organization with a roadmap for implementing its incident response capability;
- describes the structure and organization of the incident response capability;
- provides a high-level approach for how the incident response capability fits into the overall organization;
- meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- defines reportable incidents;
- provides metrics for measuring the incident response capability within the organization;
- defines the resources and management support needed to effectively maintain and mature an incident response capability;
- is reviewed and approved by designated officials within the organization.

**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 planning responsibilities.

**ASSESSMENT PROCEDURE: IR-8.2**

**Assessment Objective**

Determine if:
the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;

the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan;

the organization reviews the incident response plan in accordance with the organization-defined frequency;

the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.

**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 planning responsibilities.

# 9.0MAINTENANCE (MA) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **MA-1 – System Maintenance Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, CM-5, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system maintenance policy; | | |

the organization system maintenance policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities;

the organization develops and formally documents system maintenance procedures;

the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls;

the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities;

the organization reviews/updates the information system maintenance policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

| MA-2 – Controlled Maintenance (Moderate) | | |
|---|---|---|
| **Control**<br>The organization:<br>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;<br>b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;<br>c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;<br>d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and<br>e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.<br>**Implementation Standard(s)**<br>1. (For PII only) In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | | |
| **Guidance**<br>The control is intended to address the information security aspects of the organization's CMS information system maintenance program. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. | | |
| **Applicability:** All; Optional for SS | **Reference(s):** FISCAM: AC-6, CP-2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MA-2.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization 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; | | |

the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** Facility documentation (such as floor plan and elevation drawings) are updated when repairs and modifications cause changes to the physical components of the facility containing PII.

**Interview:** Organizational personnel with information system maintenance responsibilities.

**Interview:** Organizational personnel, with facility management responsibilities.

**MA-2(1) – Enhancement (Moderate)**

**Control**

the organization maintains maintenance records for the information system that include:
- date and time of maintenance;
- name of the individual performing the maintenance;
- name of escort, if necessary;
- a description of the maintenance performed;
- a list of equipment removed or replaced (including identification numbers, if applicable).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

| ASSESSMENT PROCEDURE: MA-2(1).1 | | |
|---|---|---|
| **Assessment Objective**<br>Determine if the organization maintains maintenance records for the information system that include:<br>- date and time of maintenance;<br>- name of the individual performing the maintenance;<br>- name of escort, if necessary;<br>- description of the maintenance performed; and<br>- list of equipment removed or replaced (including identification numbers, if applicable).<br>**Assessment Methods And Objects**<br>**Examine:** Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records. | | |
| **MA-3 – Maintenance Tools (Moderate)** | | |
| **Control**<br>The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools. | | |
| **Guidance**<br>The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping", "ls", "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, CP-2; IRS-1075: 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MA-3.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization approves, controls, and monitors the use of information system maintenance tools;<br>the organization maintains information system maintenance tools on an ongoing basis. | | |

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.

**MA-3(2) – Enhancement (Moderate)**

**Control**

The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-3(2).1**

**Assessment Objective**

Determine if the organization checks all media containing diagnostic and test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

| MA-4 – Non-Local Maintenance (Moderate) | | |
|---|---|---|
| **Control**<br>The organization prohibits non-local CMS system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:<br>a. Monitors and controls non-local maintenance and diagnostic activities;<br>b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;<br>c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;<br>d. Maintains records for non-local maintenance and diagnostic activities; and<br>e. Terminates all sessions and network connections when non-local maintenance is completed.<br>**Implementation Standard(s)**<br>1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service. | | |
| **Guidance**<br>Non-local 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. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. 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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, SM-7; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** IA-2, MP-6 |
| **ASSESSMENT PROCEDURE: MA-4.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization prohibits non-local CMS system maintenance unless explicitly authorized, in writing, by the CIO; | | |

if authorized, the organization monitors and controls non-local maintenance and diagnostic activities;

if authorized, the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools;

if authorized, the organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;

if authorized, the organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;

if authorized, the organization terminates all sessions and network connections when non-local maintenance is completed.

if authorized, the organization maintains records for non-local maintenance and diagnostic activities;

if authorized, the organization (or information system in certain cases) terminates all sessions and network connections when non-local maintenance or diagnostics is completed.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

## MA-4(1) – Enhancement (Moderate)

**Control**

The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: MA-4(1).1

**Assessment Objective**

Determine if:
the organization audits non-local maintenance and diagnostic sessions;

designated organizational personnel review the maintenance records of the sessions.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; maintenance records; audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities.

## MA-4(2) – Enhancement (Moderate)

**Control**

The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: MA-4(2).1

**Assessment Objective**

Determine if the organization documents the installation and use of non-local maintenance and diagnostic connections in the security plan for the information system.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; maintenance records; audit records; other relevant documents or records.

## MA-4(3) – Enhancement (Moderate)

**Control**

The organization:
(a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or
(b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to sensitive information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-4(3).1**

**Assessment Objective**

Determine if:
the organization requires and ensures non-local maintenance and diagnostic services from an information system that implements a level of security at least as high as the level of security implemented on the information system being serviced; or

the organization removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities;

the organization after the removed component service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting to the information system.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; service provider contracts and/or service level agreements; maintenance records; audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system maintenance responsibilities; information system maintenance provider.

**MA-5 – Maintenance Personnel (Moderate)**

**Control**

The organization:
a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and
b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

**Guidance**

Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, SM-7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-5.1**

**Assessment Objective**

Determine if:
the organization establishes a process for maintenance personnel authorization;

the organization maintains a current list of authorized maintenance organizations or personnel;

personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with information system maintenance responsibilities.

**MA-6 – Timely Maintenance (Moderate)**

**Control**

The organization obtains maintenance support and/or spare parts for CMS critical systems and applications (including Major Applications [MA] and General Support Systems [GSS] and their components) within twenty-four (24) hours of failure.

**Guidance**

The organization specifies those CMS information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-6.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, CMS critical information system and applications (including MA and GSS and their components) for which it will obtain maintenance support and/or spare parts;

the organization obtains maintenance support and/or spare parts for CMS critical information systems and applications (including MA and GSS and their components) within twenty-four (24) hours of failure.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with information system maintenance responsibilities.

# *10.0* MEDIA PROTECTION (MP) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **MP-1 – Media Protection Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.<br>**Implementation Standard(s)**<br>1. (For PII only) Semi-annual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SM-1, SM-3; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents media protection policy; | | |

the organization media protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities;

the organization develops and formally documents media protection procedures;

the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls;

the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities.

the organization reviews/updates the media protection policy and procedures within every three hundred sixty-five (365) days.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Media protection policy and procedures; other relevant documents or records.

**Examine:** PII semiannual inventory reports; other relevant documents or records.

**Interview:** Organizational personnel with information system media protection responsibilities.

**MP-2 – Media Access (Moderate)**

**Control**

The organization restricts access to CMS sensitive digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.

**Guidance**

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AC-6, BP-3; HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-2.1**

**Assessment Objective**

Determine if:
the organization defines:
- digital and non-digital media requiring restricted access;
- individuals authorized to access the media;
- security measures taken to restrict access;

the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system media protection responsibilities.

| MP-2(1) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. | | |
| **Guidance**<br>This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices). | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-2(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization employs automated mechanisms to restrict access to media storage areas;<br>the organization employs automated mechanisms to audit access attempts and access granted to media storage areas. | | |
| **Assessment Methods And Objects**<br>**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 devices; access control records; audit records; other relevant documents or records. | | |
| **MP-3 – Media Marking (Moderate)** | | |
| **Control**<br>The organization:<br>a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and<br>b. Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment. | | |

**Guidance**

The term marking is used when referring to the application or use of human-readable security attributes. The term labeling is used when referring to the application or use of security attributes with regard to internal data structures within the information system (see AC-16, Security Attributes). Removable information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Organizations may extend the scope of this control to include information system output devices containing sensitive information, including, for example, monitors and printers. Marking of removable media and information system output is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; IRS-1075: 4.6#1, 5.1#1.2, 5.3#2.1-2, 5.3#3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-3.1**

**Assessment Objective**

Determine if:
the organization defines removable media types and information system output that require marking;

the organization marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information;

the organization defines:
- removable media types and information system output exempt from marking;
- controlled areas designated for retaining removable media and information output exempt from marking;

removable media and information system output exempt from marking remain within designated controlled areas.

**Assessment Methods And Objects**

**Examine:** Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and information system output; other relevant documents or records.

**Interview:** Organizational personnel with information system media protection and marking responsibilities.

| MP-4 – Media Storage (Moderate) |
|---|
| **Control**<br>The organization:<br>a. Physically controls and securely stores digital and non-digital media within controlled areas using safeguards prescribed for the highest system security level of the information ever recorded on it;<br>b. Protects CMS information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.<br>**Implementation Standard(s)**<br>1. (For PII only) Evaluate employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance.<br>2. (For PII only) If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information. |
| **Guidance**<br>Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting CMS information and/or CMS information system.<br>An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on CMS or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection.<br>As part of a defense-in-depth strategy, the organization considers routinely encrypting CMS information at rest on selected secondary storage devices. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AC-6; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1 | **Related Controls Requirement(s):** AC-19, CP-9, CP-9(4), RA-2, SC-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-4.1**

**Assessment Objective**

Determine if:
the organization defines:
- types of digital and non-digital media physically controlled and securely stored within designated controlled areas;
- controlled areas designated to physically control and securely store the media;
- security measures to physically control and securely store the media within designated controlled areas;

the organization physically controls and securely stores CMS information system media within organization-defined controlled areas using organization-defined security measures;

the organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

the organization meets all the requirements specified in the applicable 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; security plan; information system media; other relevant documents or records.

**Examine:** Cryptographic software licenses used to protect PII at rest.

**Examine:** PII magnetic media storage procedures.

**Interview:** Organizational personnel with PII protection responsibilities.

**Interview:** Organizational personnel with information system media protection and storage responsibilities.

| MP-5 – Media Transport (Moderate) |
| --- |
| **Control**<br>The organization:<br>a. Protects and controls digital and non-digital media containing CMS sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier;<br>b. Maintains accountability for information system media during transport outside of controlled areas; and<br>c. Restricts the activities associated with transport of such media to authorized personnel.<br>**Implementation Standard(s)**<br>1. (For PII only) Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.<br>2. (For FTI only) Organizations are not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7) |

**Guidance**

Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting CMS information and/or CMS information system.

Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides: (i) the selection of media and associated information contained on that media requiring protection during transport; and (ii) the selection and use of storage containers for transporting non-digital media.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.6#2, 4.6#4 | **Related Controls**<br>**Requirement(s):** AC-19, CP-9, CP-9(4) |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-5.1**

**Assessment Objective**

Determine if:

the organization protects and controls digital and non-digital media containing CMS sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and (a) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier;

the organization maintains accountability for information system media during transport outside of controlled areas;

the organization identifies personnel authorized to transport information system media outside of controlled areas;

the organization restricts the activities associated with transport of information system media to authorized personnel.

the organization meets all the requirements specified in the applicable 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; security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records.

**Examine:** Rosters or list of authorized personnel to protect and control PII media during transit.

**Examine:** FTI disclosure documentation. (See IRS Pub. 1075, sect. 11.1 and 11.7)

**Interview:** Organizational personnel responsible for FTI disclosure.

**MP-5(1) – Enhancement (Moderate)**

**Control**

[Withdrawn: Incorporated into MP-5].

**MP-5(2) – Enhancement (Moderate)**

**Control**

The organization documents activities associated with the transport of information system media.

**Guidance**

Organizations establish documentation requirements for activities associated with the transport of CMS information system media in accordance with CMS requirements.

| **Applicability:** All | **Reference(s):** IRS-1075: 3.2#3.1, 4.4#2, 4.6#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-5(2).1**

**Assessment Objective**

Determine if the organization documents activities associated with the transport of information system media.

**Assessment Methods And Objects**

**Examine:** Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media transport records; audit records; other relevant documents or records.

**MP-5(4) – Enhancement (Moderate)**

**Control**

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

**Guidance**

This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-5(4).1**

**Assessment Objective**

Determine if the organization employs 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; other relevant documents or records.

**MP-6 – Media Sanitization (Moderate)**

**Control**

The organization:
a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

**Implementation Standard(s)**

1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.
2. (For FTI only) FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee.
3. (For PII only) Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:
- date received
- reel/cartridge control number contents
- number of records, if available
- movement, and
- if disposed of, the date and method of disposition.

**Guidance**

This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of sensitive information to unauthorized individuals when such media is reused or released for disposal. The organization uses its discretion on the employment of 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 CMS or individuals if released for reuse or disposal.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-1075: 4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2 | **Related Controls Requirement(s):** MA-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-6.1**

**Assessment Objective**

Determine if:
the organization sanitizes information system media both digital and non-digital prior to:
- disposal;
- release out of organizational control; or
- release for reuse;

the organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records.

**Examine:** FTI disposal records.

**Examine:** PII inventory tape/cartridge log.

**Interview:** Organizational personnel with information system media sanitization responsibilities.

**MP-6(1) – Enhancement (Moderate)**

**Control**

The organization tracks, documents, and verifies media sanitization and disposal actions.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-6(1).1**

**Assessment Objective**

Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.

**Assessment Methods And Objects**

**Examine:** Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records.

**Interview:** Organizational personnel with information system media sanitization responsibilities.

| MP-6(2) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization tests sanitization equipment and procedures to verify correct performance periodically. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-6(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the frequency for testing sanitization equipment and procedures to verify correct performance;<br>the organization tests sanitization equipment and procedures to verify correct performance in accordance with organization-defined frequency.<br>**Assessment Methods And Objects**<br>**Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records.<br>**Interview:** Organizational personnel with information system media sanitization responsibilities. | | |
| **MP-6(5) – Enhancement (Moderate)** | | |
| **Control**<br>The organization sanitizes information system media containing sensitive information using National Security Agency (NSA) guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, Guidelines for Media Sanitization. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-6(5).1** | | |
| **Assessment Objective**<br>Determine if the organization sanitizes information system media containing classified information in accordance with NSA standards and policies.<br>**Assessment Methods And Objects**<br>**Examine:** Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records. | | |

**Interview:** Organizational personnel with information system media sanitization responsibilities.

**MP-6(6) – Enhancement (Moderate)**

**Control**

The organization destroys media containing sensitive information that cannot be sanitized.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-6(6).1**

**Assessment Objective**

Determine if the organization implements the media destruction process for information system media that cannot be sanitized.

**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; other relevant documents or records.

**Interview:** Organizational personnel with information system media sanitization responsibilities.

**MP-CMS-1 – Media Related Records (Moderate)**

**Control**

Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.

**Implementation Standard(s)**

1. The media records must, at a minimum, contain:
(a) The name of media recipient;
(b) Signature of media recipient;
(c) Date/time media received;
(d) Media control number and contents;
(e) Movement or routing information; and
(f) If disposed of, the date, time, and method of destruction.

| | | |
|---|---|---|
| **Guidance**<br>Employing a hash function (a reproducible method of turning inventory data into a relatively small number may serve as a digital "fingerprint" of the data) for electronic inventory records maintenance so the inventory information can be validated as not being tampered with prior to reconstructive events for an investigation of a possible breach. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-CMS-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization maintains inventory and disposition records for information system media to ensure control and accountability of CMS information;<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**Examine:** Media protection policy and procedures; other relevant documents or records.<br>**Interview:** Organizational personnel with information system media protection responsibilities. | | |

# 11.0 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PE-1 – Physical and Environmental Protection Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-2, CP-2, SM-1, SM-3; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents physical and environmental protection policy; | | |

the organization physical and environmental protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities;

the organization develops and formally documents physical and environmental protection procedures;

the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls;

the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities;

the organization reviews/updates the physical and environmental protection policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with physical and environmental protection responsibilities.

## PE-2 – Physical Access Authorizations (Moderate)

**Control**

The organization:
a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
b. Issues authorization credentials;
c. Reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.

**Implementation Standard(s)**

1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days.
2. (For PII only) Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.

**Guidance**

Authorization credentials include, for example, badges, identification cards, and smart cards.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-2.1**

**Assessment Objective**

Determine if:
the organization identifies areas within the facility that are publicly accessible;

the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

the organization issues authorization credentials (e.g., badges, identification cards, smart cards).

the organization reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** Restricted areas, security rooms, or locked rooms that control access to areas containing PII.

**Interview:** Organization personnel responsible for controlling restricted areas, security rooms, or locked rooms containing PII.

| PE-3 – Physical Access Control (Moderate) |
|---|
| **Control**<br>The organization:<br>a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);<br>b. Verifies individual access authorizations before granting access to the facility;<br>c. Controls entry to the facility containing the information system using physical access devices and/or guards;<br>d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;<br>e. Controls access authorization lists to secure areas;<br>f. Secures keys, combinations, and other physical access devices;<br>g. Inventories physical access devices within every three hundred sixty-five (365) days; and<br>h. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.<br>**Implementation Standard(s)**<br>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.<br>2. Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.<br>3. Restrict access to grounds/facilities to authorized persons only.<br>4. (For PII only) 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 after hours. |
| **Guidance**<br>The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) a CMS information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SD-1, SM-4; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-3.1**

**Assessment Objective**

Determine if:
the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

the organization verifies individual access authorizations before granting access to the facility;

the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;

the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

the organization secures keys, combinations, and other physical access devices;

the organization inventories physical access devices within every three hundred sixty-five (365) days;

the organization changes combinations and keys periodically; and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** PII protection barriers.

**Interview:** Organizational personnel with physical access control responsibilities.

**PE-4 – Access Control for Transmission Medium (Moderate)**

**Control**

The organization controls physical access to information system distribution and transmission lines within organizational facilities.

**Implementation Standard(s)**

1. Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel.
2. Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use.

**Guidance**

Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-4.1**

**Assessment Objective**

Determine if:
the organization controls physical access to information system distribution and transmission lines within organizational facilities.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PE-5 – Access Control for Output Devices (Moderate)**

**Control**

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

**Guidance**

Monitors, printers, and audio devices are examples of information system output devices.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6; HIPAA: 164.310(b) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-5.1**

**Assessment Objective**

Determine if the organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; actual displays from information system components; other relevant documents or records.

**PE-6 – Monitoring Physical Access (Moderate)**

**Control**

The organization:
a. Monitors physical access to the information system to detect and respond to physical security incidents;
b. Reviews physical access logs in accordance with the frequency specified in Implementation Standard 1; and
c. Coordinates results of reviews and investigations with the organization's incident response capability.

**Implementation Standard(s)**

1. Review physical access logs every at least once every two (2) months.

**Guidance**

Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AC-6, SM-5 | **Related Controls Requirement(s):** IR-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-6.1**

**Assessment Objective**

Determine if:
the organization monitors physical access to the information system to detect and respond to physical security incidents;

the organization reviews physical access logs in accordance with the organization-defined frequency;

the organization coordinates results of reviews and investigations with the organization's incident response capability.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with physical access monitoring responsibilities.

**PE-6(1) – Enhancement (Moderate)**

**Control**

The organization monitors real-time physical intrusion alarms and surveillance equipment.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-6(1).1**

**Assessment Objective**

Determine if the organization monitors real-time physical intrusion alarms and surveillance equipment.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; other relevant documents or records.

**Interview:** Organizational personnel with physical access monitoring responsibilities.

**PE-7 – Visitor Control (Moderate)**

**Control**

The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

**Guidance**

Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6; HIPAA: 164.310(a)(2)(iii) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-7.1**

**Assessment Objective**

Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.

**Interview:** Organizational personnel with visitor access control responsibilities.

**PE-7(1) – Enhancement (Moderate)**

**Control**

The organization escorts visitors and monitors visitor activity, when required.

| | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** HIPAA: 164.310(a)(2)(iii) | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: PE-7(1).1**

**Assessment Objective**

Determine if the organization escorts visitors and monitors visitor activity, when required.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.

**Interview:** Organizational personnel with visitor access control responsibilities.

**PE-8 – Access Records (Moderate)**

**Control**

The organization:
a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
b. Closes and reviews visitor access records monthly.

**Guidance**

Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-8.1**

**Assessment Objective**

Determine if:
the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

the organization reviews the visitor access records in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for reviewing physical access records.

**PE-9 – Power Equipment and Power Cabling (Moderate)**

**Control**

The organization protects power equipment and power cabling for the information system from damage and destruction.

**Implementation Standard(s)**

1. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-9.1**

**Assessment Objective**

Determine if:
the organization protects power equipment and power cabling for the information system from damage and destruction.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PE-10 – Emergency Shutoff (Moderate)**

**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;
c. Protects emergency power shutoff capability from unauthorized activation; and
d. 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.

**Guidance**

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

| **Applicability:** All | **Reference(s):** FISCAM: CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-10.1**

**Assessment Objective**

Determine if:
the organization provides the capability of shutting off power to the information system or individual system components in emergency situations;

the organization defines the location of emergency shutoff switches or devices by information system or system component;

the organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel;

the organization protects the emergency power shutoff capability from unauthorized activation.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; other relevant documents or records.

**PE-10(1) – Enhancement (Moderate)**

**Control**

[Withdrawn: Incorporated into PE-10].

**PE-11 – Emergency Power (Moderate)**

**Control**

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-11.1**

**Assessment Objective**

Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; other relevant documents or records.

| PE-12 – Emergency Lighting (Moderate) | | |
|---|---|---|
| **Control**<br>The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. | | |
| **Guidance**<br>This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-12.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption;<br>the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility;<br>the organization maintains the automatic emergency lighting for the information system. | | |
| **Assessment Methods And Objects**<br>**Examine:** Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records.<br>**Interview:** Organizational personnel with emergency planning responsibilities. | | |
| **PE-13 – Fire Protection (Moderate)** | | |
| **Control**<br>The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. | | |

**Guidance**

Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13.1**

**Assessment Objective**

Determine if:
the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source;

the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

**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; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems.

**PE-13(1) – Enhancement (Moderate)**

**Control**

The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13(1).1**

**Assessment Objective**

Determine if the organization employs fire detection devices/systems for the information system that, without manual intervention, activate automatically and notify the organization and emergency responders in the event of a fire.

**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; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems.

**PE-13(2) – Enhancement (Moderate)**

**Control**

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13(2).1**

**Assessment Objective**

Determine if the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems.

**PE-13(3) – Enhancement (Moderate)**

**Control**

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13(3).1**

**Assessment Objective**

Determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

**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; other relevant documents or records.

**Interview:** Organizational personnel with responsibilities for fire detection and suppression devices/systems.

**PE-14 – Temperature and Humidity Controls (Moderate)**

**Control**

The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and
b. Monitors temperature and humidity levels.

**Implementation Standard(s)**

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

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: PE-14.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization defines the acceptable temperature and humidity levels within the facility where the information system resides;<br>the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels;<br>the organization defines the frequency to monitor temperature and humidity levels;<br>the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |
| **PE-15 – Water Damage Protection (Moderate)** | | |
| **Control**<br>The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. | | |
| **Guidance**<br>This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: PE-15.1**

**Assessment Objective**

Determine if:
the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly;

key personnel within the organization have knowledge of the master water shutoff values.

**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; other relevant documents or records.

**Interview:** Organization personnel with physical and environmental protection responsibilities.

**PE-16 – Delivery and Removal (Moderate)**

**Control**

The organization authorizes, monitors, and controls the flow of CMS information system-related components entering and exiting the facility and maintains records of those items.

**Guidance**

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-16.1**

**Assessment Objective**

Determine if:
the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility;

the organization maintains records of information system components entering and exiting the facility.

**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; 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 (Moderate)

**Control**

The organization:
a. Employs appropriate security controls at alternate work sites to include, but not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems;
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.

**Guidance**

Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2; HIPAA: 164.310(a)(2)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-17.1**

**Assessment Objective**

Determine if:
the organization defines the management, operational, and technical information system security controls to be employed at alternate work sites;

the organization employs organization-defined management, operational, and technical information system security controls at alternate work sites;

the organization assesses, as feasible, the effectiveness of security controls at alternate work sites;

the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.

**Assessment Methods And Objects**

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

**Interview:** Organization personnel using alternate work sites.

## PE-18 – Location of Information System Components (Moderate)

**Control**

The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

**Guidance**

Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2; HIPAA: 164.312(c)(1) | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: PE-18.1

**Assessment Objective**

Determine if:
the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards;

the organization positions information system components within the facility to minimize the opportunity for unauthorized access.

**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; other relevant documents or records.

# 12.0 PLANNING (PL) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PL-1 – Security Planning Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PL-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security planning policy; | | |

the organization security planning policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities;

the organization develops and formally documents security planning procedures;

the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls;

the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities;

the organization reviews/updates the security planning policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Security planning policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with security planning responsibilities.

## PL-2 – System Security Plan (SSP) (Moderate)

**Control**

The organization:
a. Develops a security plan for the information system that:
- Is consistent with the CMS System Security Plan (SSP) Procedure;
- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the operational environment for the information system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and
c. 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 due to changes in the threat environment; or
- Before the previous security authorization expires.

**Implementation Standard(s)**

1. (For PHI only) 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).)
2. (For FTI only) When FTI is incorporated into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition to those specified in other controls.
3. (For FTI only) Develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7 & 8)

**Guidance**

The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to CMS operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended.

All CMS information systems and major applications are covered by an SSP, which is compliant with current CMS SSP Procedures.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, CP-1, CP-2, SM-1; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PL-2.1**

**Assessment Objective**

Determine if:
the organization develops a security plan for the information system that:
- is consistent with the organization's enterprise architecture;
- explicitly defines the authorization boundary for the system;
- describes the operational context of the information system in terms of mission and business processes;
- provides the security categorization of the information system including supporting rationale;
- describes the operational environment for the information system;
- describes relationships with or connections to other information systems;
- provides an overview of the security requirements for the system;
- describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions;
- is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

the organization defines the frequency of security plan reviews;

the organization reviews the security plan in accordance with the organization-defined frequency, minimally every three (3) years;

the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Examine:** Sampling of policies and procedures relating to 164.306 for retention period. (See HIPAA 164.316(b))

**Examine:** Compliance controls if FTI is incorporated into a Data Warehouse. (See IRS Pub 1075 Exhibit 7)

**Examine:** SPRs and SARs..

**Examine:** Procedures that document who obtains documentation and which documentation pertains to whom for implementation.

**Interview:** Organization personnel with security planning and plan implementation responsibilities for the information system.

**Interview:** Organizational personnel with retention responsibilities related to 164.306. (See HIPAA 164.316(b))

**Interview:** Organizational personnel who are responsible for implementation of procedures to determine if documentation is available.

**PL-3 – System Security Plan Update (Moderate)**

**Control**

[Withdrawn: Incorporated into PL-2].

**PL-4 – Rules of Behavior (ROB) (Moderate)**

**Control**

The organization:
a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information, information system, and network use; and
b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

**Guidance**

The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior.
ROBs are aligned with DHHS requirements posted at http://hhs.gov/ocio/policy/2008-0001.003s.html, and made readily available.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, SM-4; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PL-4.1**

**Assessment Objective**

Determine if:
the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;

the organization makes the rules available to all information system users;

the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

**Assessment Methods And Objects**

**Examine:** Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records.

**Interview:** Organizational personnel who are authorized users of the information system and have signed rules of behavior.

**PL-5 – Privacy Impact Assessment (PIA) (Moderate)**

**Control**

The organization conducts a Privacy Impact Assessment (PIA) on the information system in accordance with OMB policy.

| | | |
|---|---|---|
| **Applicability:** All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC | **Reference(s):** FISCAM: SM-5; HSPD 7: J(35) | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: PL-5.1**

**Assessment Objective**

Determine if:
the organization conducts a privacy impact assessment on the information system;

the privacy impact assessment is in accordance with OMB policy.

**Assessment Methods And Objects**

**Examine:** Security planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records.

**PL-6 – Security-Related Activity Planning (Moderate)**

**Control**

The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on CMS operations (i.e., mission, functions, image, and reputation), CMS assets, and individuals.

**Guidance**

Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.

| **Applicability:** All | **Reference(s):** FISCAM: SM-1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PL-6.1**

**Assessment Objective**

Determine if the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

**Assessment Methods And Objects**

**Examine:** Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records.

**Interview:** Organizational personnel with security planning and plan implementation responsibilities.

# 13.0 PERSONNEL SECURITY (PS) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PS-1 – Personnel Security Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SD-2, SM-1, SM-3, SM-4; IRS-1075: 5.6.2.1#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PS-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents personnel security policy; | | |

the organization personnel security policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities;

the organization develops and formally documents personnel security procedures;

the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls;

the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities;

the organization reviews/updates the personnel security policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Personnel security policy and procedures, other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

**PS-2 – Position Categorization (Moderate)**

**Control**

The organization:
a. Assigns a criticality/sensitivity risk designation to all positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and revises position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.

**Guidance**

Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).

| **Applicability:** All | **Reference(s):** FISCAM: SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: PS-2.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization assigns a risk designations to all positions within the organization;<br>the organization establishes a screening criteria for individuals filling organizational positions;<br>the organization defines in the security plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions;<br>the organization reviews/revises position risk designations within every three hundred sixty-five (365) days.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records.<br>**Interview:** Organizational personnel with personnel security responsibilities. | | |
| **PS-3 – Personnel Screening (Moderate)** | | |
| **Control**<br>The organization:<br>a. Screens individuals prior to authorizing access to the information system; and<br>b. Rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position.<br>**Implementation Standard(s)**<br>1. Perform criminal history check for all persons prior to employment.<br>2. Require appropriate personnel to obtain and hold a moderate-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook. | | |
| **Guidance**<br>Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. For prospective employees, references background checks are performed before issuance of a User ID. Security agreements are required for employees and contractors assigned to work with mission critical information. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SM-4, SM-7; IRS-1075: 5.6.2.1#1.4 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: PS-3.1**

**Assessment Objective**

Determine if:
the organization screens individuals prior to authorizing access to the information system;

the organization rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position;

the personnel screening is consistent with 5 CFR 731.106, OPM policy, regulations, and guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

**PS-4 – Personnel Termination (Moderate)**

**Control**

The organization, upon termination of individual employment:
a. Revokes system and physical access immediately following employee termination;
b. Conducts exit interviews;
c. Retrieves all security-related CMS information system-related property;
d. Retains access to CMS information and information systems formerly controlled by terminated individual; and
e. Immediately escorts employees terminated for cause out of the organization.

**Implementation Standard(s)**

1. System access must be revoked prior to or during the employee termination process.

**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 individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all CMS information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and nonavailability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause. Appropriate personnel have access to official records created by the terminated employee that are stored on CMS information systems.

| **Applicability:** All | **Reference(s):** FISCAM: SM-4; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: 5.6.2.1#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-4.1**

**Assessment Objective**

Determine if:

the organization terminates information system access upon termination of individual employment;

the organization conducts exit interviews of terminated personnel;

the organization retrieves all security-related CMS information system-related property from terminated personnel;

the organization, upon termination of individual employment, retrieves all security-related CMS information system-related property;

the organization, upon termination of individual employment, retains access to CMS information and information systems formerly controlled by terminated individual;

the organization, upon termination of individual employment, immediately escorts employees terminated for cause out of the organization.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

| PS-5 – Personnel Transfer (Moderate) | | |
|---|---|---|
| **Control**<br>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 the following transfer or reassignment actions during the formal transfer process:<br>a. Re-issuing appropriate CMS information system-related property (e.g., keys, identification cards, building passes);<br>b. Notification to security management;<br>c. Closing obsolete accounts and establishing new accounts; and<br>d. Revocation of all system access privileges (if applicable). | | |
| **Guidance**<br>This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts. | | |
| **Applicability:** All | **Reference(s):** FISCAM: SM-4; IRS-1075: 5.6.2.1#1.6 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PS-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization;<br>the organization defines the transfer or reassignment actions and the time period within which the actions must occur following formal transfer or reassignment;<br>the organization initiates the organization-defined transfer or reassignment actions within an organization-defined time period following formal transfer or reassignment. | | |

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities.

**PS-6 – Access Agreements (Moderate)**

**Control**

The organization:
a. Ensures that individuals requiring access to CMS information or information systems sign appropriate access agreements prior to being granted access; and
b. Reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended.

**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 the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-6.1**

**Assessment Objective**

Determine if:
the organization identifies appropriate access agreements for individuals requiring access to CMS information and information systems;

individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access;

the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates for access agreements;

the organization reviews/updates the access agreements in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with personnel security responsibilities.

## PS-7 – Third-Party Personnel Security (Moderate)

**Control**

The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Documents personnel security requirements; and
c. Monitors provider compliance.

**Implementation Standard(s)**

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 CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies and standards.

**Guidance**

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. Security requirements include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SD-1, SM-4, SM-7; IRS-1075: 5.6.2.1#1.8 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: PS-7.1

**Assessment Objective**

Determine if:
the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers;

the organization documents personnel security requirements for third-party providers;

the organization monitors third-party provider compliance with personnel security requirements.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with personnel security responsibilities; third-party providers.

**PS-8 – Personnel Sanctions (Moderate)**

**Control**

The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

**Guidance**

The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, SD-2, SM-4; HIPAA: 164.308(a)(1)(ii)(C) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-8.1**

**Assessment Objective**

Determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

**Assessment Methods And Objects**

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

**Interview:** Organizational personnel with personnel security responsibilities.

# 14.0 RISK ASSESSMENT (RA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **RA-1 – Risk Assessment Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-2, SM-3; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075: 5.6.1.1#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: RA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents risk assessment policy; | | |

the organization risk assessment policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities;

the organization develops and formally documents risk assessment procedures;

the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls;

the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities;

the organization reviews/updates the risk assessment policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with risk assessment responsibilities.

**RA-2 – Security Categorization (Moderate)**

**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 designated representative.

**Guidance**

A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to CMS operations, CMS assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the CMS CIO, CISO, Business Owner, senior information security officer, and information owners/stewards. The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted.
All CMS information systems categorized as High or Moderate are considered sensitive or to contain sensitive information. All CMS information systems categorized as Low are considered non-sensitive or to 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.

| **Applicability:** All | **Reference(s):** FISCAM: CP-1, SM-2; HSPD 7: D(8); IRS-1075: 4.1#2 | **Related Controls Requirement(s):** MP-4, SC-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-2.1**

**Assessment Objective**

Determine if:
the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

the organization documents the security categorization results (including supporting rationale) in the security plan for the information system;

the CMS authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

**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; other relevant documents or records.

**Interview:** Organizational personnel with security categorization and risk assessment responsibilities.

| RA-3 – Risk Assessment (Moderate) |
|---|
| **Control**<br>The organization:<br>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;<br>b. Documents risk assessment results in accordance with the CMS Information Security (IS) Risk Assessment (RA) Procedures;<br>c. Reviews risk assessment results within every three hundred sixty-five (365) days; and<br>d. Updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. |
| **Guidance**<br>A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to CMS operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to CMS operations, CMS assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing CMS information systems, outsourcing entities).<br>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. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems.<br>Risk assessments can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the baselines with additional security controls or control enhancements. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-5, CP-1, CP-2, SM-2; HIPAA: 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3, 6.3.3#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-3.1**

**Assessment Objective**

Determine if:
the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:
- access;
- use;
- disclosure;
- disruption;
- modification; or
- destruction;

the organization documents risk assessment results in accordance with the CMS IS RA Procedures;

the organization reviews risk assessment results within every three hundred sixty-five (365) days;

the organization updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records.

**Interview:** Organizational personnel with risk assessment responsibilities.

**RA-4 – Risk Assessment Update (Moderate)**

**Control**

[Withdrawn: Incorporated into RA-3].

| RA-5 – Vulnerability Scanning (Moderate) |
|---|
| **Control**<br>The organization:<br>a. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:<br>- Enumerating platforms, software flaws, and improper configurations;<br>- Formatting and making transparent, checklists and test procedures; and<br>- Measuring vulnerability impact;<br>b. Analyzes vulnerability scan reports and results from security control assessments;<br>c. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and<br>d. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).<br>**Implementation Standard(s)**<br>1. Scans for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported.<br>2. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with CMS IS procedures. |
| **Guidance**<br>The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan. |

| **Applicability:** All | **Reference(s):** FISCAM: CM-5, SM-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5.1**

**Assessment Objective**

Determine if:
the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:
- enumerating platforms, software flaws, and improper configurations;
- formatting/and making transparent checklists and test procedures;
- measuring vulnerability impact;

the organization analyzes vulnerability scan reports and results from security control assessments;

the organization remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk;

the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.

**Interview:** Organizational personnel with risk assessment and vulnerability scanning responsibilities.

**RA-5(1) – Enhancement (Moderate)**

**Control**

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5(1).1**

**Assessment Objective**

Determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; records of updates to vulnerabilities scanned; other relevant documents or records.

# 15.0 SYSTEM AND SERVICES ACQUISITION (SA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| SA-1 – System and Services Acquisition Policy and Procedures (Moderate) |
|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.<br>**Implementation Standard(s)**<br>1. (For FTI only) Develop, disseminates, and periodically reviews/updates a formal, documented, system and services acquisition policy that includes IRS documents received and identified by:<br>(a) Taxpayer name<br>(b) Tax year(s)<br>(c) Type of information (e.g., revenue agent reports, Form 1040, work papers)<br>(d) The reason for the request<br>(e) Date requested<br>(f) Date received<br>(g) Exact location of the FTI<br>(h) Who has had access to the data and<br>(i) If disposed of, the date and method of disposition. |

**Guidance**

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.1.3#1.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-1.1**

**Assessment Objective**

Determine if:

the organization develops and formally documents system services and acquisition policy;

the organization system services and acquisition policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system services and acquisition policy to elements within the organization having associated system services and acquisition roles and responsibilities;

the organization develops and formally documents system services and acquisition procedures;

the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls;

the organization disseminates formal documented system services and acquisition procedures to elements within the organization having associated system services and acquisition roles and responsibilities;

the organization reviews/updates the system services and acquisition policy and procedures within every three hundred sixty-five (365) days.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** System and services acquisition policy and procedures; other relevant documents or records.

**Examine:** Organizational documentation that contains the development, dissemination, and review/updates to FTI IRS documents received.

**Interview:** Organizational personnel with system and services acquisition responsibilities.

## SA-2 – Allocation of Resources (Moderate)

**Control**

The organization:
a. Includes a determination of information security requirements for the information system in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system 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' programming and budgeting documentation for the implementation and management of information systems security.

| **Applicability:** All | **Reference(s):** FISCAM: CM-3, IN-2, SD-1, SM-1 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: SA-2.1

**Assessment Objective**

Determine if:
the organization includes a determination of the information security requirements for the information system in mission/business process planning;

the organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process;

the organization establishes a discrete line item for information security in organizational programming and budgeting documentation;

the organization establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security.

**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 – Life Cycle Support (Moderate)**

**Control**

The organization:
a. Manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS Integrated IT Investment & System Life Cycle Framework (ILC);
b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
c. Identifies individuals having information system security roles and responsibilities.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-3, AS-5, BP-1, BP-2, BP-3, BP-4, CM-1, CM-3, CP-3, DA-1, IN-1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-3.1**

**Assessment Objective**

Determine if:
the organization manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS Integrated IT Investment & System Life Cycle Framework (ILC);

the organization defines and documents information system security roles and responsibilities throughout the system development life cycle;

the organization identifies individuals having information system security roles and responsibilities.

**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 – Acquisitions (Moderate)**

**Control**

The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
a. Security functional requirements/specifications;
b. Security-related documentation requirements; and
c. Developmental and evaluation-related assurance requirements.

**Implementation Standard(s)**

1. Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

**Guidance**

The acquisition documents for CMS information systems, CMS information system components, and CMS information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.

Solicitation Documents:

Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required:

- Security capabilities;
- Design and development processes;
- Test and evaluation procedures; and
- Documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

Use of Evaluated and Validated Products:

For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources:

1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-3, SM-7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-4.1**

**Assessment Objective**

Determine if:
the organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
- security functional requirements/specifications;
- security-related documentation requirements;
- developmental and evaluation-related assurance requirements.

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 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) – Enhancement (Moderate)**

**Control**

The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-4(1).1**

**Assessment Objective**

Determine if the organization requires in acquisition documents that vendors/contractors provide information describing in the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.

**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(4) – Enhancement (Moderate)**

**Control**

The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-4(4).1**

**Assessment Objective**

Determine if:
the organization explicitly assigns each acquired information system component to an information system;

the owner of the system acknowledges each assignment of information system components to the information system.

**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; information system owner.

| SA-5 – Information System Documentation (Moderate) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:<br>- Secure configuration, installation, and operation of the information system;<br>- Effective use and maintenance of security features/functions; and<br>- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and<br>b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:<br>- User-accessible security features/functions and how to effectively use those security features/functions;<br>- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and<br>- User responsibilities in maintaining the security of the information and information system; and<br>c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.<br>**Implementation Standard(s)**<br>1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.<br>2. Maintain an updated list of related system operations and security documentation.<br>3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. | | |
| **Guidance**<br>The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, AS-3, AS-4, AS-5, BP-1, BP-2, BP-3, BP-4, CM-2, CM-3, CP-2, DA-1, IN-1, IN-2, SD-1, SD-2; IRS-1075: 5.6.1.3#1.3 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: SA-5.1**

**Assessment Objective**

Determine if:
the organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
- secure configuration, installation, and operation of the information system;
- effective use and maintenance of the security features/functions;
- known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

the organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
- user-accessible security features/functions and how to effectively use those security features/functions;
- methods for user interaction with the information system, which enables individuals to use the system in a more secure manner;
- user responsibilities in maintaining the security of the information and information system;

the organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

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 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.

**ASSESSMENT PROCEDURE: SA-5.FIS-1**

**Assessment Objective**

Determine if:
the organization develops information system documentation for operating the system that includes:
- operational instructions and
- appropriate end user control, balancing, and verification features and procedures.

the organization disseminates information system documentation to appropriate elements within the organization;

responsible parties within the organization periodically review information system documentation;

the organization updates information system documentation when organizational review indicates updates are required or changes are made to the system.

**Assessment Methods And Objects**

**Examine:** Information system documentation; other relevant documents or records.

**Interview:** Organizational management and personnel with information system operations, control, and user responsibilities.

**SA-5(1) – Enhancement (Moderate)**

**Control**

The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-5(1).1**

**Assessment Objective**

Determine if:
the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation;

the documentation describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

**Assessment Methods And Objects**

**Examine:** System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records.

**Interview:** Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system.

| SA-5(3) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. | | |
| **Guidance**<br>An information system can be partitioned into multiple subsystems. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-5(3).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation;<br>the documentation describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. | | |
| **Assessment Methods And Objects**<br>**Examine:** System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records.<br>**Interview:** Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system. | | |

| SA-6 – Software Usage Restrictions (Moderate) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Uses software and associated documentation in accordance with contract agreements and copyright laws;<br>b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and<br>c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. | | |
| **Guidance**<br>Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization. | | |
| **Applicability:** All | **Reference(s):** FISCAM: CM-3, CM-5; IRS-1075: 4.7.3#1.2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-6.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization uses software and associated documentation in accordance with contract agreements and copyright laws;<br>the organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution;<br>the organization 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. | | |
| **Assessment Methods And Objects**<br>**Examine:** System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records.<br>**Interview:** Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system. | | |

| SA-7 – User-Installed Software (Moderate) | | |
|---|---|---|
| **Control**<br>The organization prohibits users from downloading or installing software, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, explicit rules govern the installation of software by users.<br>**Implementation Standard(s)**<br>1. If user installed software is authorized, ensure that business rules and technical controls enforce the documented authorizations and prohibitions. | | |
| **Guidance**<br>If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). | | |
| **Applicability:** All | **Reference(s):** FISCAM: CM-3, CM-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-7.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users;<br>the organization (or information system) enforces explicit rules governing the installation of software by users.<br>the organization meets all the requirements specified in the applicable implementation standard(s). | | |
| **Assessment Methods And Objects**<br>**Examine:** System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records.<br>**Interview:** Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system. | | |

| SA-8 – Security Engineering Principles (Moderate) | | |
|---|---|---|
| **Control**<br>The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. | | |
| **Guidance**<br>The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of 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 into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions. | | |
| **Applicability:** All | **Reference(s):** FISCAM: BP-2, BP-4, CM-3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-8.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization applies information system security engineering principles in the specification of the information system;<br>the organization applies information system security engineering principles in the design of the information system;<br>the organization applies information system security engineering principles in the development of the information system;<br>the organization applies information system security engineering principles in the implementation of the information system;<br>the organization applies information system security engineering principles in the modification of the information system. | | |

**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 (Moderate)**

**Control**

The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Monitors security control compliance by external service providers.
d. Prohibits service providers from outsourcing any system function outside the U.S. or its territories.

**Implementation Standard(s)**

1. (For PHI only) A covered entity under HIPAA may permit a business associate to 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. (See HIPAA 164.308(b) and 164.314(a).)

**Guidance**

An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization 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 to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-7; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4 | **Related Controls Requirement(s):** CA-3 |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-9.1**

**Assessment Objective**

Determine if:

the organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services;

the organization monitors security control compliance by external service providers.

the organization prohibits service providers from outsourcing any system function outside the U.S. or its territories.

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; other relevant documents or records.

**Examine:** Business associate assurance documentation. (See HIPAA 164.308(b) and 164.314(a))

**Interview:** Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

**Interview:** Organizational personnel responsible for maintaining business associate assurance documentation. (See HIPAA 164.308(b) and 164.314(a))

**SA-10 – Developer Configuration Management (Moderate)**

**Control**

The organization requires that information system developers/integrators:
a. Perform configuration management during information system design, development, implementation, and operation;
b. Manage and control changes to the information system;
c. Implement only organization-approved changes;
d. Document approved changes to the information system; and
e. Track security flaws and flaw resolution.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-3, BP-2, BP-4, CM-3, CM-4, CM-6, CP-2, DA-1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-10.1**

**Assessment Objective**

Determine if:
the organization requires that information system developers/integrators:

perform configuration management during information system:
- design;
- development;
- implementation;
- operation;

manage and control changes to the information system during:
- design;
- development;
- implementation;
- modification;

implement only organization-approved changes;

document approved changes to the information system;

track security flaws and flaw resolution.

**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 (Moderate)**

**Control**

The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):
a. Create and implement a security test and evaluation plan in accordance with, but not limited to the, current CMS procedures;
b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security control assessment process; and
c. Document the results of the security control assessment and flaw remediation processes.

**Implementation Standard(s)**

1. If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results.
2. Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.

**Guidance**

Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-3, CM-3, SM-5 | **Related Controls Requirement(s):** CA-2, CA-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-11.1**

**Assessment Objective**

Determine if:
the organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):
- create and implement a security test and evaluation plan in accordance with, but not limited to the, current CMS procedures;
- implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
- document the results of the security testing/evaluation and flaw remediation processes.

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 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.

# 16.0 SYSTEM AND COMMUNICATIONS PROTECTION (SC) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **SC-1 – System and Communications Protection Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-5, SM-1, SM-3; IRS-1075: 5.6.3.4#1, 5.6.3.4#2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system and communications protection policy; | | |

the organization system and communications protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities;

the organization develops and formally documents system and communications protection procedures;

the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls;

the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities;

the organization reviews/updates the system and communications protection policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy and procedures; other relevant documents or records.

**Interview:** Organizational personnel with system and communications protection responsibilities.

**SC-2 – Application Partitioning (Moderate)**

**Control**

The information system separates user functionality (including user interface services [e.g., web services]) from information system management (e.g., database management systems) functionality.

**Guidance**

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AS-2, DA-1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-2.1**

**Assessment Objective**

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.

**SC-4 – Information in Shared Resources (Moderate)**

**Control**

The information system prevents unauthorized and unintended information transfer via shared system resources.

**Implementation Standard(s)**

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.
2. (For FTI only) When authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

**Guidance**

The purpose of this control is to prevent sensitive information, including encrypted representations of sensitive information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remnence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the CMS information system for which there is only a single user/role.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; IRS-1075: 5.6.3.4#2, 5.6.3.4#3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-4.1**

**Assessment Objective**

Determine if:
the information system prevents unauthorized and unintended information transfer via shared system resources.

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 remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**Examine:** Bulk record identities that have been transmitted externally.

| SC-5 – Denial of Service Protection (Moderate) | | |
|---|---|---|
| **Control**<br>The information system protects against or limits the effects of the following types of denial of service attacks defined on the following sites or in the following documents:<br>- SANS Organization www.sans.org/dosstep;<br>- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and<br>- NIST CVE List http://checklists.nist.gov/home.cfm. | | |
| **Guidance**<br>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 devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines in the security plan, explicitly or by reference, the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system;<br>the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks. | | |
| **Assessment Methods And Objects**<br>**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. | | |

| SC-7 – Boundary Protection (Moderate) | | |
|---|---|---|
| **Control**<br>The information system:<br>a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and<br>b. Connects to external networks or information systems only through managed interfaces consisting of automated boundary protection devices arranged in accordance with an organizational security architecture.<br>**Implementation Standard(s)**<br>1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.<br>2. Utilize stateful inspection/application firewall hardware and software.<br>3. Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network. | | |
| **Guidance**<br>Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ).<br>The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. When this situation occurs, the organization implements appropriate compensating security controls. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AS-2 | **Related Controls Requirement(s):** AC-4, CA-3, MP-4, RA-2 |

**ASSESSMENT PROCEDURE: SC-7.1**

**Assessment Objective**

Determine if:
the organization defines the external boundary of the information system;

the organization defines key internal boundaries of the information system;

the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system;

the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

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 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; other relevant documents or records.

**Interview:** Selected organizational personnel with boundary protection responsibilities.

**SC-7(1) – Enhancement (Moderate)**

**Control**

The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.

**Guidance**

Publicly accessible information system components include, for example, public web servers.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(1).1**

**Assessment Objective**

Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.

**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.

**SC-7(2) – Enhancement (Moderate)**

**Control**

The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(2).1**

**Assessment Objective**

Determine if:
the organization defines the mediation necessary for public access to the organization's internal networks;

the information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records.

**SC-7(3) – Enhancement (Moderate)**

**Control**

The organization limits the number of access points to the information system (e.g., prohibiting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

**Guidance**

Desktop modems allow backdoors into the network, putting the data and network at very high risk. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(3).1**

**Assessment Objective**

Determine if the organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

**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) – Enhancement (Moderate)**

**Control**

The organization:
(a) Implements a managed interface for each external telecommunication service;
(b) Establishes a traffic flow policy for each managed interface;
(c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
(e) Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days; and
(f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

**Guidance**

"External telecommunication services" addresses transmissions of data to/from entities external to the secure site, including to other secure sites using networks or any other communication resources outside of the physical control of the secure site to transmit information.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(4).1**

**Assessment Objective**

Determine if:
the organization implements a managed interface for each external telecommunication service;

the organization establishes a traffic flow policy for each managed interface;

the organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;

the organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;

the organization reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days;

the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

**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; other relevant documents or records.

**Interview:** Selected organizational personnel with boundary protection responsibilities.

**SC-7(5) – Enhancement (Moderate)**

**Control**

The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(5).1**

**Assessment Objective**

Determine if:
the information system, at managed interfaces, denies network traffic by default;

the information system, at managed interfaces, allows network traffic by exception.

**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(6) – Enhancement (Moderate)**

**Control**

The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(6).1**

**Assessment Objective**

Determine if:
the organization prevents the unauthorized release of information outside of the information system boundary; or

the organization prevents any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

**Assessment Methods And Objects**

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

**SC-7(7) – Enhancement (Moderate)**

**Control**

The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

**Guidance**

This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent split-tunneling. Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7(7).1**

**Assessment Objective**

Determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

**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.

**SC-8 – Transmission Integrity (Moderate)**

**Control**

The information system protects the integrity of transmitted information.

**Implementation Standard(s)**

1. Employ appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13).

**Guidance**

This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization implements appropriate compensating security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.312(c)(1) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-8.1**

**Assessment Objective**

Determine if:
the information system protects the integrity of transmitted information.

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 transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**SC-8(1) – Enhancement (Moderate)**

**Control**

The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

**Guidance**

Alternative physical protection measures include, for example, protected distribution systems.

| **Applicability:** All | **Reference(s):** HIPAA: 164.312(c)(1) | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: SC-8(1).1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.<br>**Assessment Methods And Objects**<br>**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. | | |
| **SC-9 – Transmission Confidentiality (Moderate)** | | |
| **Control**<br>The information system protects the confidentiality of transmitted information.<br>**Implementation Standard(s)**<br>1. (For PII only) When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information. | | |
| **Guidance**<br>This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization implements appropriate compensating security controls. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, BP-2, BP-4; HIPAA: 164.312(e)(1); IRS-1075: 5.6.3.4#2, 5.6.3.4#4.1 | **Related Controls**<br>**Requirement(s):** AC-17 |

| **ASSESSMENT PROCEDURE: SC-9.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the information system protects the confidentiality of transmitted information.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records.<br>**Examine:** Fax machine locations for secure custodial coverage of outgoing and incoming PII transmitted data. | | |
| **SC-9(1) – Enhancement (Moderate)** | | |
| **Control**<br>The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. | | |
| **Guidance**<br>Alternative physical protection measures include, for example, protected distribution systems. | | |
| **Applicability:** All | **Reference(s):** HIPAA: 164.312(e)(1), 164.312(e)(2)(ii); IRS-1075: 5.6.3.4#2, 5.7#1 | **Related Controls**<br>**Requirement(s):** SC-13 |
| **ASSESSMENT PROCEDURE: SC-9(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization optionally defines alternative physical measures to prevent unauthorized disclosure of information during transmission;<br>the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by organization-defined alternative physical measures. | | |

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

**SC-10 – Network Disconnect (Moderate)**

**Control**

The information system automatically terminates the network connection associated with a communications session at the end of the session, or:
a. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and
b. Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity.

**Guidance**

This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.
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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AS-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-10.1**

**Assessment Objective**

Determine if:
the information system automatically terminates a network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity; or

the information system:
- forcibly de-allocates communications session DHCP leases after seven (7) days; and
- forcibly disconnects inactive VPN connections after thirty (30) minutes of inactivity.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.

## SC-12 – Cryptographic Key Establishment and Management (Moderate)

**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.

**Guidance**

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; IRS-1075: 5.7.1#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-12.1**

**Assessment Objective**

Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.

**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.

## SC-13 – Use of Cryptography (Moderate)

**Control**

When cryptographic mechanisms are used, the information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

| | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2, 5.6.3.4#4.2-3 | **Related Controls Requirement(s):** AC-3, SC-8.Std.1, SC-9(1) |

**ASSESSMENT PROCEDURE: SC-13.1**

**Assessment Objective**

Determine if when cryptographic mechanisms are used, the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**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; other relevant documents or records.

**SC-13(1) – Enhancement (Moderate)**

**Control**

When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.

| | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: SC-13(1).1**

**Assessment Objective**

Determine if when cryptographic mechanisms are used, the organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

| SC-14 – Public Access Protections (Moderate) | | |
|---|---|---|
| **Control**<br>The information system protects the integrity and availability of publicly available information and applications.<br>**Implementation Standard(s)**<br>1. Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.<br>2. If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix D: E-authentication Standard. | | |
| **Guidance**<br>The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.<br>CMS refers to the National Institute of Standards and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix D: E-authentication Standard provides a summary for remote access controls. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-14.1** | | |
| **Assessment Objective**<br>Determine if:<br>the information system protects the integrity and availability of publicly available information and applications.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. | | |

| SC-15 – Collaborative Computing Devices (Moderate) | | |
|---|---|---|
| **Control**<br>The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system:<br>a. Prohibits remote activation of collaborative computing devices; and<br>b. Provides an explicit indication of use to users physically present at the devices. | | |
| **Guidance**<br>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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-15.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative;<br>if authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used;<br>if authorized, the information system prohibits remote activation of collaborative computing devices;<br>if authorized, the information system provides an explicit indication of use to users physically present at the devices. | | |
| **Assessment Methods And Objects**<br>**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. | | |

| SC-15(1) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-15(1).1** | | |
| **Assessment Objective**<br>Determine if the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.<br>**Assessment Methods And Objects**<br>**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. | | |
| **SC-17 – Public Key Infrastructure Certificates (Moderate)** | | |
| **Control**<br>The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. | | |
| **Guidance**<br>This control focuses on certificates with a visibility external to the CMS information system and does not include certificates related to internal system operations, for example, application-specific time services. Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: SC-17.1**

**Assessment Objective**

Determine if the organization issues public key certificates under the organization-defined certificate policy or obtains public key certificates under a certificate policy from an approved service provider.

**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 (Moderate)**

**Control**

The organization:
a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

**Guidance**

Decisions regarding the employment of mobile code within CMS information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on CMS servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-18.1**

**Assessment Objective**

Determine if:
the organization defines acceptable and unacceptable mobile code and mobile code technologies;

the organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies;

the organization authorizes, monitors, and controls the use of mobile code within the information system.

**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.

## SC-19 – Voice Over Internet Protocol (Moderate)

**Control**

The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If authorized, the organization:
a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

| **Applicability:** All | **Reference(s):** FISCAM: CM-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-19.1**

**Assessment Objective**

Determine if:
the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously;

the organization authorizes, monitors, and controls the use of VoIP within the information system.

**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.

| SC-20 – Secure Name /Address Resolution Service (Authoritative Source) (Moderate) | | |
|---|---|---|
| **Control**<br>The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. | | |
| **Guidance**<br>This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. 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. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-20.1** | | |
| **Assessment Objective**<br>Determine if the information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. | | |
| **SC-20(1) – Enhancement (Moderate)** | | |
| **Control**<br>The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains. | | |

**Guidance**

An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-20(1).1**

**Assessment Objective**

Determine if:
the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces;

the information system, when operating as part of a distributed, hierarchical namespace, enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**SC-22 – Architecture and Provisioning for Name /Address Resolution Service (Moderate)**

**Control**

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

**Guidance**

A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).

| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-22.1**

**Assessment Objective**

Determine if:
the information systems that collectively provide name/address resolution service for an organization are fault tolerant;

the information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.

**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.

## SC-23 – Session Authenticity (Moderate)

**Control**

The information system provides mechanisms to protect the authenticity of communications sessions.

**Guidance**

This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-23.1**

**Assessment Objective**

Determine if the information system provides mechanisms to protect the authenticity of communications sessions.

**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.

**SC-28 – Protection of Information at Rest (Moderate)**

**Control**

The information system protects the confidentiality and integrity of information at rest.

**Guidance**

This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within a CMS information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-28.1**

**Assessment Objective**

Determine if the information system protects the confidentiality and integrity of information at rest.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records.

**SC-32 – Information System Partitioning (Moderate)**

**Control**

The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

**Guidance**

Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-32.1**

**Assessment Objective**

Determine if the organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

**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 (Moderate)**

**Control**

Controls shall be implemented to protect CMS sensitive information that is sent via email.

**Implementation Standard(s)**

1. Prior to sending an email, place all CMS sensitive information in an encrypted attachment.

**Guidance**

A good place to obtain recommended security practices for handling sensitive information via e-mail is NIST SP 800-45 (as amended), Guidelines on Electronic Mail Security.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: SC-CMS-1.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization effectively implements protections for CMS sensitive information that is sent via e-mail;<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**Examine:** Email policy and procedures; other relevant documents or records.<br>**Interview:** Sample of organizational personnel who use email. | | |
| **SC-CMS-2 – Website Usage (Moderate)** | | |
| **Control**<br>CMS web sites are operated within the restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction. | | |
| **Guidance**<br>Monitor the CMS and DHHS security programs to determine is there are any modified directives and instruction. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-CMS-2.1** | | |
| **Assessment Objective**<br>Determine if the organization maintains CMS websites within restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction.<br>**Assessment Methods And Objects**<br>**Examine:** CMS web site baseline and change management documentation for appropriate configurations.<br>**Interview:** Web site administrators. | | |

# 17.0 SYSTEM AND INFORMATION INTEGRITY (SI) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **SI-1 – System and Information Integrity Policy and Procedures (Moderate)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, BP-1, BP-2, BP-3, BP-4, CP-2, SM-1, SM-3; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system and information integrity policy; | | |

the organization system and information integrity policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities;

the organization develops and formally documents system and information integrity procedures;

the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls;

the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities.

the organization reviews/updates the system and information integrity policy and procedures within every three hundred sixty-five (365) days.

**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 (Moderate)**

**Control**

The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software updates related to flaw remediation for effectiveness and potential side effects on CMS information systems before installation; and
c. Incorporates flaw remediation into the organizational configuration management process.

**Implementation Standard(s)**

1. Correct identified information system flaws on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days.
(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.

**Guidance**

The organization identifies CMS information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) installs security-relevant software updates (e.g., patches, service packs, and hot fixes) within the CMS-designated time period. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in CMS information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts have been accomplished.

| **Applicability:** All | **Reference(s):** FISCAM: AS-3, CM-5; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls**<br>**Requirement(s):** CA-2, CA-4, CA-7, CM-3, IR-4, SI-11 |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-2.1**

**Assessment Objective**

Determine if:
the organization identifies, reports, and corrects information system flaws;

the organization tests software updates related to flaw remediation for effectiveness before installation;

the organization tests software updates related to flaw remediation for potential side effects on organizational information systems before installation;

the organization incorporates flaw remediation into the organizational configuration management process.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with flaw remediation responsibilities.

**SI-2(1) – Enhancement (Moderate)**

**Control**

The organization centrally manages the flaw remediation process and installs software updates automatically.

**Guidance**

Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-2(1).1**

**Assessment Objective**

Determine if:
the organization centrally manages the flaw remediation process;

the organization installs software updates automatically.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic 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; other relevant documents or records.

| SI-2(2) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation. | | |
| **Applicability:** All | **Reference(s):** HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-2(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation;<br>the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |

| SI-3 – Malicious Code Protection (Moderate) |
| --- |
| **Control**<br>The organization:<br>a. Employs malicious code protection mechanisms at CMS information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:<br>- Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or<br>- Inserted through the exploitation of information system vulnerabilities;<br>b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with CMS configuration management policy and procedures;<br>c. Configures malicious code protection mechanisms to:<br>- Perform critical system file scans during system boot, information system scans using the frequency specified in Implementation Standard 1, and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and<br>- Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and<br>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.<br>**Implementation Standard(s)**<br>1. Desktop malicious code scanning software is configured to perform critical system file scans every twenty (24) hours. |

**Guidance**

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong 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 CMS missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

| **Applicability:** All | **Reference(s):** FISCAM: CM-5; IRS-1075: 5.6.2.5#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-3.1**

**Assessment Objective**

Determine if:

the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code:

- transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- inserted through the exploitation of information system vulnerabilities;

the organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

- transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- inserted through the exploitation of information system vulnerabilities;

the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1;

the organization defines one or more of the following actions to be taken in response to malicious code detection:
- block malicious code;
- quarantine malicious code; and/or
- send alert to administrator;

the organization configures malicious code protection mechanisms to:
- perform periodic scans of the information system in accordance with organization-defined frequency;
- perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;
- take organization-defined action(s) in response to malicious code detection;

the organization addresses the receipt of false positives during malicious code:
- detection and eradication;
- the resulting potential impact on the availability of the information system.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with malicious code protection responsibilities.

**SI-3(1) – Enhancement (Moderate)**

**Control**

The organization centrally manages malicious code protection mechanisms.

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.5#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-3(1).1**

**Assessment Objective**

Determine if the organization centrally manages malicious code protection mechanisms.

**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) – Enhancement (Moderate)

**Control**

The information system automatically updates malicious code protection mechanisms (including signature definitions).

| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.5#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: SI-3(2).1

**Assessment Objective**

Determine if the information system automatically updates malicious code protection mechanisms, including signature definitions.

**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(3) – Enhancement (Moderate)

**Control**

The information system prevents non-privileged users from circumventing malicious code protection capabilities.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: SI-3(3).1

**Assessment Objective**

Determine if the information system prevents non-privileged users from circumventing malicious code protection capabilities.

**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 (Moderate)**

**Control**

The organization:
a. Monitors events on the information system in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks;
b. Identifies unauthorized use of the information system;
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and
e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

**Implementation Standard(s)**

1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.

**Guidance**

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). 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, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at 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. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, DA-1, SM-5; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4 | **Related Controls Requirement(s):** AC-8, AU-4, CM-6 |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4.1**

**Assessment Objective**

Determine if:

the organization monitors events on the information system in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks;

the organization identifies unauthorized use of the information system;

the organization deploys monitoring devices:
- strategically within the information system to collect organization-determined essential information;
- at ad hoc locations within the system to track specific types of transactions of interest to the organization;

the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**Interview:** Organizational personnel with information system monitoring responsibilities.

**SI-4(1) – Enhancement (Moderate)**

**Control**

The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4(1).1**

**Assessment Objective**

Determine if the organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

**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; other relevant documents or records.

**SI-4(2) – Enhancement (Moderate)**

**Control**

The organization employs automated tools to support near real-time analysis of events.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

| ASSESSMENT PROCEDURE: SI-4(2).1 | | |
|---|---|---|
| **Assessment Objective**<br>Determine if the organization employs automated tools to support near real-time analysis of events.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |
| **SI-4(4) – Enhancement (Moderate)** | | |
| **Control**<br>The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. | | |
| **Guidance**<br>Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components. | | |
| **Applicability:** All | **Reference(s):** IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-4(4).1** | | |
| **Assessment Objective**<br>Determine if:<br>the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.<br>the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. | | |

**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; other relevant documents or records.

**SI-4(5) – Enhancement (Moderate)**

**Control**

The information system provides near real-time alerts when the following indications of compromise or potential compromise occur:
(a) Presence of malicious code,
(b) Unauthorized export of information,
(c) Signaling to an external information system, or
(d) Potential intrusions.

**Guidance**

Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4(5).1**

**Assessment Objective**

Determine if:
the organization defines indicators of compromise or potential compromise to the security of the information system;
the information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

| SI-4(6) – Enhancement (Moderate) | | |
|---|---|---|
| **Control**<br>The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-4(6).1** | | |
| **Assessment Objective**<br>Determine if the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |
| **SI-5 – Security Alerts, Advisories, and Directives (Moderate)** | | |
| **Control**<br>The organization:<br>a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;<br>b. Generates internal security alerts, advisories, and directives as deemed necessary;<br>c. Disseminates security alerts, advisories, and directives to appropriate personnel; and<br>d. Implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance. | | |

**Guidance**

Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) 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 affects on CMS operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-3, CM-5, DA-1, SM-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-5.1**

**Assessment Objective**

Determine if:
the organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;

the organization generates internal security alerts, advisories, and directives;

the organization defines personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives;

the organization disseminates security alerts, advisories, and directives to organization-identified personnel;

the organization implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records.

**Interview:** Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system.

**SI-7 – Software and Information Integrity (Moderate)**

**Control**

The information system detects unauthorized changes to software and information.

**Guidance**

The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices consistent with CMS information security policy and procedures with regard to commercial-off-the-shelf (COTS) integrity mechanisms, and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications. Integrity mechanisms include, but are not limited to, parity checks, check-sums, error detection data validation techniques, cyclical redundancy checks, and cryptographic hashes to detect and protect against information tampering, errors, omissions and unauthorized changes to software.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, CM-4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-7.1**

**Assessment Objective**

Determine if the information system detects unauthorized changes to software and information.

**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.

**SI-7(1) – Enhancement (Moderate)**

**Control**

The organization reassesses the integrity of software and information by performing daily integrity scans of the information system.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-7(1).1**

**Assessment Objective**

Determine if the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.

**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-8 – Spam Protection (Moderate)**

**Control**

The organization:
a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with CMS configuration management policy and procedures.

**Guidance**

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers.

| **Applicability:** All | **Reference(s):** FISCAM: CM-5; HIPAA: 164.308(a)(1)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-8.1**

**Assessment Objective**

Determine if:
the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means;

the organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means;

the organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1.

**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.

**SI-8(1) – Enhancement (Moderate)**

**Control**

The organization centrally manages spam protection mechanisms.

| **Applicability:** All | **Reference(s):** HIPAA: 164.308(a)(1)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-8(1).1**

**Assessment Objective**

Determine if the organization centrally manages spam protection mechanisms.

**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-9 – Information Input Restrictions (Moderate)**

**Control**

The organization restricts the capability to input information to the information system to authorized personnel.

**Guidance**

Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

| **Applicability:** All | **Reference(s):** FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.1 | **Related Controls Requirement(s):** |
|---|---|---|

| ASSESSMENT PROCEDURE: SI-9.1 | | |
|---|---|---|
| **Assessment Objective**<br>Determine if the organization restricts the capability to input information to the information system to authorized personnel.<br>**Assessment Methods And Objects**<br>**Examine:** System and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.<br>**Interview:** Organizational personnel with responsibilities for implementing restrictions on individual authorizations to input information into the information system. | | |
| **SI-10 – Information Input Validation (Moderate)** | | |
| **Control**<br>The information system uses automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. | | |
| **Guidance**<br>Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. | | |
| **Applicability:** All | **Reference(s):** FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; IRS-1075: 5.6.2.5#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-10.1** | | |
| **Assessment Objective**<br>Determine if the information system uses automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.<br>**Assessment Methods And Objects**<br>**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. | | |

| SI-11 – Error Handling (Moderate) | | |
|---|---|---|
| **Control**<br>The information system:<br>a. Identifies potentially security-relevant error conditions;<br>b. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries; and<br>c. Reveals error messages only to authorized personnel. | | |
| **Guidance**<br>The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, User IDs, account numbers, social security numbers, and credit card numbers. | | |
| **Applicability:** All | **Reference(s):** FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2 | **Related Controls Requirement(s):** SI-2 |
| **ASSESSMENT PROCEDURE: SI-11.1** | | |
| **Assessment Objective**<br>Determine if:<br>the information system identifies potentially security-relevant error conditions;<br>the organization defines sensitive or potentially harmful information that should not be contained in error logs and administrative messages;<br>the information system generates error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries;<br>the information system reveals error messages only to authorized personnel. | | |
| **Assessment Methods And Objects**<br>**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. | | |

| SI-12 – Information Output Handling and Retention (Moderate) | | |
|---|---|---|
| **Control**<br>The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.<br>**Implementation Standard(s)**<br>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 National Archives and Records Administration (NARA) requirements. | | |
| **Guidance**<br>The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention. | | |
| **Applicability:** All | **Reference(s):** FISCAM: BP-2, BP-3; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-12.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization handles both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements;<br>the organization retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**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.<br>**Interview:** Organizational personnel with information output handling and retention responsibilities. | | |

# CMS Information Security (IS)
# Acceptable Risk Safeguards (ARS)

## Appendix C - CMSR Low Impact Level Data

***(Rev.1, 05-24-11)***

## Table of Contents


1.0 Access Control (AC) – Technical 1

2.0 Awareness and Training (AT) – Operational 29

3.0 Audit and Accountability (AU) – *Technical* 35

4.0 Security Assessment and Authorization (CA) – *Management* 48

5.0 Configuration Management (CM) – *Operational* 63

6.0 Contingency Planning (CP) – *Operational* 71

7.0 Identification and Authentication (IA) – *Technical* 81

8.0 Incident Response (IR) – *Operational* 92

9.0 Maintenance (MA) – *Operational* 102

*10.0* Media Protection (MP) – *Operational* 108

11.0 Physical and Environmental Protection (PE) – *Operational* 113

12.0 Planning (PL) – *Management* 125

13.0 Personnel Security (PS) – *Operational* 131

14.0 Risk Assessment (RA) – *Management* 140

15.0 System and Services Acquisition (SA) – *Management* 147

16.0 System and Communications Protection (SC) – *Technical* 159

17.0 System and Information Integrity (SI) – *Operational* 170

# 1.0 ACCESS CONTROL (AC) – TECHNICAL

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **AC-1 – Access Control Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AS-1, SM-1, SM-3; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents access control policy; | | |

the organization access control policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities;

the organization develops and formally documents access control procedures;

the organization access control procedures facilitate implementation of the access control policy and associated access controls;

the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities;

the organization reviews/updates the access control policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Access control policy and procedures; other relevant documents or records.

| AC-2 – Account Management (Low) | | |
|---|---|---|
| **Control**<br>The organization manages information system accounts, including:<br>a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);<br>b. Establishing conditions for group membership;<br>c. Identifying authorized users of the information system and specifying access privileges;<br>d. Requiring appropriate approvals for requests to establish accounts;<br>e. Establishing, activating, modifying, disabling, and removing accounts;<br>f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;<br>g. Notifying account managers 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;<br>h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;<br>i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and<br>j. Reviewing accounts using the frequency specified in Implementation Standard 1.<br>**Implementation Standard(s)**<br>1. Review information system accounts within every three hundred sixty-five (365) days and require annual certification.<br>2. Remove or disable default user accounts. Rename active default accounts.<br>3. Implement centralized control of user access administrator functions.<br>4. Regulate the access provided to contractors and define security requirements for contractors. | | |
| **Guidance**<br>The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AC-4, AS-2, AS-4, BP-3, SD-2, SM-4; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: AC-2.1**

**Assessment Objective**

Determine if:
the organization manages information system accounts, including;
- identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
- establishing conditions for group membership;
- identifying authorized users of the information system and specifying access privileges;
- requiring appropriate approvals for requests to establish accounts;
- establishing, activating, modifying, disabling, and removing accounts;
- specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- notifying account managers 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;
- deactivating: (a) temporary accounts that are no longer required; and (b) accounts of terminated or transferred users;
- granting access to the system based on: (a) a valid access authorization; (b) intended system usage; and (c) other attributes as required by the organization or associated missions/business functions;

the organization reviews information system accounts in accordance with the frequency specified in Implementation Standard 1.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing account management; security plan; list of active 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.

**AC-2(3) – Enhancement (Low)**

**Control**

The information system automatically disables inactive accounts after three hundred sixty-five (365) days.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** IA-4.Std.1 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-2(3).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, a time period after which the information system disables inactive accounts;

the information system automatically disables inactive accounts after organization-defined time period.

**Assessment Methods And Objects**

**Examine:** Procedures addressing account management; 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; other relevant documents or records.

**AC-2(7) – Enhancement (Low)**

**Control**

The organization:
(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;
(b) Tracks and monitors privileged role assignments; and
(c) Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that unauthorized accounts have not been created.

**Guidance**

Privileged roles include, for example, key management, network and system administration, database administration, web administration.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-2(7).1**

**Assessment Objective**

Determine if:
the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;

the organization tracks and monitors privileged role assignments;

the organization inspects administrator groups, root accounts and other system related accounts on demand, but at least once during the specified period to ensure that unauthorized accounts have not been created.

**Assessment Methods And Objects**

**Examine:** Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; information system audit records; audit tracking and monitoring reports; other relevant documents or records.

**AC-3 – Access Enforcement (Low)**

**Control**

The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

**Implementation Standard(s)**

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).
2. If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix D: E-authentication Standard.
3. Configure operating system controls to disable public "write" access to files, objects, and directories that may directly impact system functionality and/or performance.

**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) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

Encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AS-1, AS-2, AS-3, AS-4, BP-2, BP-4, CM-3, DA-1, IN-2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3 | **Related Controls Requirement(s):** SC-13 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-3.1**

**Assessment Objective**

Determine if:

the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records.

| AC-3(1) – Enhancement (Low) | | |
|---|---|---|
| **Control**<br>[Withdrawn: Incorporated into AC-6]. | | |
| **AC-5 – Separation of Duties (Low)** | | |
| **Control**<br>The organization:<br>a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;<br>b. Documents separation of duties; and<br>c. Implements separation of duties through assigned information system access authorizations.<br>**Implementation Standard(s)**<br>1. Ensure that audit functions are not performed by security personnel responsible for administering access control.<br>2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities.<br>3. Ensure that critical mission functions and information system support functions are divided among separate individuals.<br>4. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups. | | |
| **Guidance**<br>Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, AS-3, AS-4, BP-4, SD-1, SD-2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion; | | |

the organization documents separation of duties;

the organization implements separation of duties through assigned information system access authorizations.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system audit records; other relevant documents or records.

## AC-6 – Least Privilege (Low)

**Control**

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

**Implementation Standard(s)**

1. Disable all file system access not explicitly required for system, application, and administrator functionality.
2. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.
3. Restrict the use of database management utilities to only authorized database administrators.
4. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If authorized, boot access is password protected.

**Guidance**

The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to CMS operations and assets, individuals, other organizations, and the Nation.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AS-2, AS-3; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); HSPD 7: D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2 | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: AC-6.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. | | |
| **AC-6(1) – Enhancement (Low)** | | |
| **Control**<br>The organization explicitly authorizes access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals. | | |
| **Guidance**<br>Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-6(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; | | |

the organization explicitly authorizes access to the organization-defined security functions and security-relevant information.

**Assessment Methods And Objects**

**Examine:** Access control policy; 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; other relevant documents or records.

**AC-6(2) – Enhancement (Low)**

**Control**

The organization requires that users of information system accounts, or roles, with access to administrator accounts or 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.

**Guidance**

This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy such as Role Based Access Control (RBAC) is being implemented 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. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-6(2).1**

**Assessment Objective**

Determine if:

the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access;

the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions;

the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions.

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

## AC-7 – Unsuccessful Login Attempts (Low)

**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 after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

**Implementation Standard(s)**

1. Configure the information system to disable access for at least five (5) minutes after three (3) failed log-on attempts by a user during a five (5) minute time period.

**Guidance**

Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2; IRS-1075: 5.6.3.2#4.1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-7.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid login attempts occur;

the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period;

the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:
- lock out the account/node for a specified time period;
- lock out the account/note until released by an administrator; or
- delay the next login prompt according to organization-defined delay algorithm;

the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded;

the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing unsuccessful login attempts; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

## AC-8 – System Use Notification (Low)

**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 for CMS information systems is:

- You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  * You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information 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 information system.
  * Any communication or data transiting or stored on this information 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: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

**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 CMS 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, web sites, web pages where substantial personal information from the public is collected, ftp, telnet, or other services accessed.

System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2 | **Related Controls Requirement(s):** SI-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-8.1**

**Assessment Objective**

Determine if:

the information system displays the CMS-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 and states that:

- users are accessing a U.S. Government information system;
- system usage may be monitored, recorded, and subject to audit;
- unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- use of the system indicates consent to monitoring and recording;

the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system;

the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; other relevant documents or records.

**ASSESSMENT PROCEDURE: AC-8.2**

**Assessment Objective**

Determine if:
the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access;

the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities;

the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.

**Assessment Methods And Objects**

**Examine:** Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.

**AC-12 – Session Termination (Low)**

**Control**

[Withdrawn: Incorporated into SC-10].

**AC-13 – Supervision and Review--Access Control (Low)**

**Control**

[Withdrawn: Incorporated into AC-2 and AU-6].

| AC-14 – Permitted Actions without Identification or Authentication (Low) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication; and<br>b. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication. | | |
| **Guidance**<br>This control is intended for public websites and other publicly available systems. It is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as http://www.usa.gov). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login 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 being repeated, but rather to situations where identification and/or authentication have not yet occurred. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AS-2 | **Related Controls Requirement(s):** IA-2 |
| **ASSESSMENT PROCEDURE: AC-14.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization identifies specific user actions that can be performed on the information system without identification or authentication;<br>the organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. | | |

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records.

**AC-15 – Automated Marking (Low)**

**Control**

[Withdrawn: Incorporated into MP-3].

**AC-17 – Remote Access (Low)**

**Control**

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Documents allowed methods of remote access to the information system;
b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
c. Monitors for unauthorized remote access to the information system;
d. Authorizes remote access to the information system prior to connection; and
e. Enforces requirements for remote connections to the information system.

**Implementation Standard(s)**

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.
2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix D: E-authentication Standard.

**Guidance**

This control requires explicit authorization prior to allowing remote access to a CMS information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to a CMS information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network (VPN) when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to CMS information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AC-4; IRS-1075: 5.6.3.2#5, 5.7.1#1 | **Related Controls**<br>**Requirement(s):** IA-2, SC-9 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-17.1**

**Assessment Objective**

Determine if:

the organization documents allowed methods of remote access to the information system;

the organization establishes usage restrictions and implementation guidance for each allowed remote access method;

the organization monitors for unauthorized remote access to the information system;

the organization authorizes remote access to the information system prior to connection;

the organization enforces requirements for remote connections to the information system.

the organization meets all the requirements specified in the applicable 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; information system audit records; other relevant documents or records.

| AC-17(7) – Enhancement (Low) | | |
|---|---|---|
| **Control**<br>The organization ensures that remote sessions used for remote administration employ additional security measures (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled) and the CMS-approved encryption standard (see SC-13). | | |
| **Guidance**<br>Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-17(7).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the security functions and security-relevant information that can be accessed using remote sessions;<br>the organization defines the additional security measures to be employed for remote sessions used to access organization-defined security functions and security-relevant information;<br>the organization employs the CMS-approved encryption standard (see SC-13) for remote sessions used to access organization-defined security functions and security-relevant information;<br>the organization audits remote sessions for accessing organization-defined security functions and security-relevant information, if required by the control. | | |
| **Assessment Methods And Objects**<br>**Examine:** Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records (if auditing is required); other relevant documents or records. | | |

| AC-18 – Wireless Access (Low) | | |
|---|---|---|
| **Control**<br>The organization prohibits the installation of wireless access points (WAP) to CMS information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If authorized, the organization:<br>a. Monitors for unauthorized wireless access to the information system; and<br>b. Enforces requirements for wireless connections to the information system.<br>**Implementation Standard(s)**<br>1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented:<br>(a) Encryption protection is enabled;<br>(b) Access points are placed in secure areas;<br>(c) Access points are shut down when not in use (i.e., nights, weekends);<br>(d) A firewall is implemented between the wireless network and the wired infrastructure;<br>(e) MAC address authentication is utilized;<br>(f) Static IP addresses, not DHCP, is utilized;<br>(g) Personal firewalls are utilized on all wireless clients;<br>(h) File sharing is disabled on all wireless clients;<br>(i) Intrusion detection agents are deployed on the wireless side of the firewall; and<br>(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis. | | |
| **Guidance**<br>Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AC-4 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-18.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization establishes usage restrictions and implementation guidance for wireless access; | | |

the organization monitors for unauthorized wireless access to the information system;

the organization authorizes wireless access to the information system prior to connection;

the organization enforces requirements for wireless connections to the information system.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records.

## AC-19 – Access Control for Mobile Devices (Low)

**Control**

The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants [PDA], cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:

a. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;

b. Monitors for unauthorized connections of mobile devices to CMS information systems;

c. Enforces requirements for the connection of mobile devices to CMS information systems;

d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and

f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

**Guidance**

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to 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). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay. Organizational policies and procedures for mobile devices 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 measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures 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 family.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1; IRS-1075: 4.6#1 | **Related Controls Requirement(s):** MP-4, MP-5 |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-19.1**

**Assessment Objective**

Determine if:

the organization prohibits the connection of portable and mobile devices to the information system unless explicitly authorized, in writing, by the CIO;

if authorized, the organization employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;

if authorized, the organization monitors for unauthorized connections of mobile devices to organizational information systems;

if authorized, the organization enforces requirements for the connection of mobile devices to organizational information systems;

if authorized, the organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

if authorized, the organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures;

if authorized, the organization defines the inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be of significant risk;

if authorized, the organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

**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; other relevant documents or records.

## AC-20 – Use of External Information Systems (Low)

**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 CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall 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 virtual private networking (VPN) and 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 Standard(s)**

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.

**Guidance**

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular 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. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies.

This control does not apply to the use of external information systems to access public interfaces to CMS information systems and information (e.g., individuals accessing federal information through www.medicare.gov). The organization establishes terms and conditions for the use of external information systems in accordance with CMS security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the CMS information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17.

| **Applicability:** All | **Reference(s):** FISCAM: SM-7; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AC-20.1**

**Assessment Objective**

Determine if:
the organization prohibits the use of external information systems to store, access, transmit, or process sensitive information unless explicitly authorized, in writing, by the CIO;

if authorized, the organization identifies individuals authorized to:
- access the information system from the external information systems;
- process, store, and/or transmit organization-controlled information using the external information systems;

if authorized, the terms and conditions address, at a minimum:
- the types of applications that can be accessed from external information systems;
- the maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
- how other users of the external information system will be prevented from accessing federal information;
- the use of virtual private networking (VPN) and firewall technologies;
- the use of and protection against the vulnerabilities of wireless technologies;
- the maintenance of adequate physical security controls;
- the use of virus and spyware protection software; and
- how often the security capabilities of installed software are to be updated.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.

| AC-22 – Publicly Accessible Content (Low) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Designates individuals authorized to post information onto a CMS information system that is publicly accessible;<br>b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;<br>c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the CMS information system;<br>d. Reviews the content on the publicly accessible CMS information system for nonpublic information monthly; and<br>e. Removes nonpublic information from the publicly accessible CMS information system, if discovered. | | |
| **Guidance**<br>Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on a CMS information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-CMS information systems is covered by appropriate organizational policy. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AC-22.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization designates individuals authorized to post information onto a CMS information system that is publicly accessible;<br>the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;<br>the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the CMS information system;<br>the organization reviews the content on the publicly accessible CMS information system for nonpublic information monthly;<br>the organization removes nonpublic information from the publicly accessible CMS information system, if discovered. | | |

**Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records; other relevant documents or records.

# 2.0AWARENESS AND TRAINING (AT) – OPERATIONAL

*(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)*

| AT-1 – Security Awareness and Training Policy and Procedures (Low) | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular CMS information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SM-1, SM-3, SM-7; IRS-1075: 5.6.2.7#1.1-2, 6.1#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AT-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security awareness and training policy; | | |

the organization security awareness and training policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities, and compliance;

the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities;

the organization develops and formally documents security awareness and training procedures;

the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls;

the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities;

the organization reviews/updates the security awareness and training policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy and procedures; other relevant documents or records.

**AT-2 – Security Awareness (Low)**

**Control**

The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by system changes, and within every three hundred sixty-five (365) days thereafter.

**Guidance**

The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the CMS information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to CMS' information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SM-4; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AT-2.1**

**Assessment Objective**

Determine if:
the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually;

the organization provides refresher security awareness training in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records.

**AT-3 – Security Training (Low)**

**Control**

The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) refresher training within every three hundred sixty-five (365) days thereafter.

**Implementation Standard(s)**

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 system changes; and refresher training within every three hundred sixty-five (365) days thereafter.

**Guidance**

The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of CMS and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of CMS' information security program.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-4; IRS-1075: 5.6.2.7#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AT-3.1**

**Assessment Objective**

Determine if:

the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes;

the organization provides role-based security-related refresher training within every three hundred sixty-five (365) days thereafter.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records.

**AT-4 – Security Training Records (Low)**

**Control**

The organization:

a. Documents and monitors individual CMS information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for three (3) years.

**Guidance**

Procedures and training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
1) All users of CMS information systems must be exposed to security awareness materials at least annually. 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 basics and policy level training in security planning and management.
3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) 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.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-4; IRS-1075: 6.2#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: AT-4.1**

**Assessment Objective**

Determine if:
the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training;

the organization retains individual training records in accordance with the organization-defined time period.

**Assessment Methods And Objects**

**Examine:** Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.

# 3.0AUDIT AND ACCOUNTABILITY (AU) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **AU-1 – Audit and Accountability Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular CMS information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, SM-1, SM-3; IRS-1075: 5.6.3.3#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents audit and accountability policy; | | |

the organization audit and accountability policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities;

the organization develops and formally documents audit and accountability procedures;

the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls;

the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities.

the organization reviews/updates the audit and accountability policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy and procedures; other relevant documents or records.

## AU-2 – Auditable Events (Low)

**Control**

The organization:
a. Determines, based on a risk assessment and CMS mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
c. Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

**Implementation Standard(s)**

1. Generate audit records for the following events:
(a) User account management activities,
(b) System shutdown,
(c) System reboot,
(d) System errors,
(e) Application shutdown,
(f) Application restart,
(g) Application errors,
(h) File creation, and
(i) File deletion.
2. Enable logging for perimeter devices, including firewalls and routers.
(a) Log packet screening denials originating from untrusted networks,
(b) Packet screening denials originating from trusted networks,
(c) User account management,
(d) Modification of packet filters,
(e) Application errors,
(f) System shutdown and reboot, and
(g) System errors.
3. Verify that proper logging is enabled in order to audit administrator activities.

**Guidance**

The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system 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 extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AC-5, AS-2, DA-1; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1 | **Related Controls Requirement(s):** AU-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-2.1**

**Assessment Objective**

Determine if:

the organization determines, based on a risk assessment and CMS mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;

the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events;

the organization provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;

the organization defines in the security plan, explicitly or by reference, information system auditable events;

the organization defines the subset of auditable events defined in (a) that are to be audited within the information system and (b) the frequency of (or situation requiring) auditing for each identified event;

the organization determines, based on current threat information and ongoing assessment of risk, the subset of auditable events defined in (a) to be audited within the information system, and (b) the frequency of (or situation requiring) auditing for each identified event.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records.

**AU-2(1) – Enhancement (Low)**

**Control**

[Withdrawn: Incorporated into AU-12].

**AU-2(2) – Enhancement (Low)**

**Control**

[Withdrawn: Incorporated into AU-12].

| AU-3 – Content of Audit Records (Low) | | |
|---|---|---|
| **Control**<br>The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. | | |
| **Guidance**<br>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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-2, DA-1; IRS-1075: 5.6.3.3#3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-3.1** | | |
| **Assessment Objective**<br>Determine if the information system produces audit records that contain sufficient information to, at a minimum, establish:<br>- what type of event occurred;<br>- when (date and time) the event occurred;<br>- where the event occurred;<br>- the source of the event;<br>- the outcome (success or failure) of the event;<br>- the identity of any user/subject associated with the event. | | |
| **Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |
| **AU-4 – Audit Storage Capacity (Low)** | | |
| **Control**<br>The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. | | |

**Guidance**

The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.3.3#4 | **Related Controls**<br>**Requirement(s):** AU-2, AU-5, AU-6, AU-7, SI-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-4.1**

**Assessment Objective**

Determine if:
the organization allocates audit record storage capacity;

the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**AU-5 – Response to Audit Processing Failures (Low)**

**Control**

The information system:
a. Alerts designated organizational officials in the event of an audit processing failure; and
b. Takes the following additional actions in response to an audit failure or audit storage capacity issue:
- Shutdown the information system,
- Stop generating audit records, or
- Overwrite the oldest records, in the case that storage media is unavailable.

**Guidance**

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, DA-1 | **Related Controls**<br>**Requirement(s):** AU-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-5.1**

**Assessment Objective**

Determine if:
the organization defines designated organizational officials to be alerted in the event of an audit processing failure;

the organization defines in the security plan, explicitly or by reference, personnel to be notified in case of an audit processing failure;

the organization defines additional actions to be taken in the event of an audit processing failure;

the information system takes the additional organization-defined actions in the event of an audit processing failure.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

**AU-6 – Audit Review, Analysis, and Reporting (Low)**

**Control**

The organization:
a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

**Implementation Standard(s)**

1. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment.
2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment.
3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
4. Use automated utilities to review audit records at least once every fourteen (14) days for unusual, unexpected, or suspicious behavior.
5. Inspect administrator groups on demand but no less than once every thirty (30) days to ensure unauthorized administrator accounts have not been created.

**Guidance**

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to CMS operations, CMS assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AC-4, AC-5, AS-2, DA-1, SM-5; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1 | **Related Controls Requirement(s):** AU-4, IR-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: AU-6.1**

**Assessment Objective**

Determine if:

the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency;

the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

the organization report findings of inappropriate/unusual activities, to designated organizational officials.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**ASSESSMENT PROCEDURE: AU-6.2**

**Assessment Objective**

Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit review, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

**AU-6(2) – Enhancement (Low)**

**Control**

[Withdrawn: Incorporated into SI-4].

**AU-8 – Time Stamps (Low)**

**Control**

The information system uses internal system clocks to generate time stamps for audit records.

**Guidance**

Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: AU-8.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if the information system uses internal system clocks to generate time stamps for audit records.<br>**Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. | | |
| **AU-9 – Protection of Audit Information (Low)** | | |
| **Control**<br>The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | | |
| **Guidance**<br>Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-9.1** | | |
| **Assessment Objective**<br>Determine if the information system protects audit information and audit tools from unauthorized:<br>- access;<br>- modification;<br>- deletion.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |

| AU-11 – Audit Record Retention (Low) | | |
|---|---|---|
| **Control**<br>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. | | |
| **Guidance**<br>The organization retains 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. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-11.1** | | |
| **Assessment Objective**<br>Determine if:<br>the retention period for audit records is consistent with the records retention policy;<br>the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.<br>**Assessment Methods And Objects**<br>**Examine:** Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; information system audit records; other relevant documents or records. | | |

| AU-12 – Audit Generation (Low) | | |
|---|---|---|
| **Control**<br>The information system:<br>a. Provides audit record generation capability for the following events in addition to those specified in other controls:<br>- All successful and unsuccessful authorization attempts.<br>- All changes to logical access control authorities (e.g., rights, permissions).<br>- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.<br>- The audit trail shall capture the enabling or disabling of audit report generation services.<br>- The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).<br>b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and<br>c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. | | |
| **Guidance**<br>Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: AU-12.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2;<br>the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2;<br>the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; | | |

the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

**Assessment Methods And Objects**

**Examine:** Audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

# 4.0SECURITY ASSESSMENT AND AUTHORIZATION (CA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CA-1 – Security Assessment and Authorization Policies and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security assessment and authorization family [formerly called Certification and Accreditation [C&A] family and process). The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 5.6.1.4#1.1-2 | **Related Controls Requirement(s):** CA-6 |
| **ASSESSMENT PROCEDURE: CA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security assessment and authorization policy; | | |

the organization security assessment and authorization policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities;

the organization develops and formally documents security assessment and authorization procedures;

the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls;

the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities;

the organization reviews/updates the security assessment and authorization policies and procedures within every three hundred sixty-five (365) days;

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policies and procedures; other relevant documents or records.

## CA-2 – Security Assessments (Low)

**Control**

The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system 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 the security requirements for the system;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

**Implementation Standard(s)**

1. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems.
2. The annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period.
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, ISSO).

**Guidance**

The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by CMS, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the FISMA annual assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring. The organization establishes 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 provided that the results are current, valid, and relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-3, SM-5; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1 | **Related Controls**<br>**Requirement(s):** CA-4, CA-6, CA-7, CA-7(1), CA-7(2), SA-11, SI-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-2.1**

**Assessment Objective**

Determine if:
the organization develops a security assessment plan for the information system;

the security assessment plan describes the scope of the assessment including:
- security controls and control enhancements under assessment;
- assessment procedures to be used to determine security control effectiveness;
- assessment environment, assessment team, and assessment roles and responsibilities.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Security assessment policy; procedures addressing security assessments; security plan; security assessment plan; assessment evidence; other relevant documents or records.

**ASSESSMENT PROCEDURE: CA-2.2**

**Assessment Objective**

Determine if:
the organization assesses the security controls in the information system within every three hundred sixty-five (365) days in accordance with the CMS IS ARS Including 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 the security requirements for the system;

the organization provides the results of the security control assessment within every 365 days, in writing, to the Business Owner;

the Business Owner reviews the assessment documentation and updates system security documentation where necessary to reflect any changes to the system;

the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records.

| CA-3 – Information System Connections (Low) |
|---|
| **Control**<br>The organization:<br>a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;<br>b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and<br>c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.<br>**Implementation Standard(s)**<br>1. Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location. |
| **Guidance**<br>This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between CMS and a nonfederal (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, SM-1; HSPD 7: F(19) | **Related Controls Requirement(s):** SA-9, SC-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-3.1**

**Assessment Objective**

Determine if:
the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);

the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;

the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated;

the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.

the organization meets all the requirements specified in the applicable 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; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records.

**CA-4 – Security Certification (Low)**

**Control**

[Withdrawn: Incorporated into CA-2].

| CA-5 – Plan of Action and Milestones (POA&M) (Low) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Develops and submits a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and<br>b. Updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. | | |
| **Guidance**<br>The POA&M is a key document in the security authorization package and is subject to federal reporting requirements established by OMB. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-5, SM-6; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4 | **Related Controls Requirement(s):** CA-7 |
| **ASSESSMENT PROCEDURE: CA-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops a plan of action and milestones for the information system within thirty (30) days of the final results for every internal/external audit/review or test;<br>the plan of action and milestones documents 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;<br>the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates;<br>the organization updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. | | |
| **Assessment Methods And Objects**<br>**Examine:** Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records. | | |

| CA-5(1) – Enhancement (Low) | | |
|---|---|---|
| **Control**<br>The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CA-5(1).1** | | |
| **Assessment Objective**<br>Determine if the organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is:<br>- accurate;<br>- up to date;<br>- readily available.<br>**Assessment Methods And Objects**<br>**Examine:** Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; plan of action and milestones; other relevant documents or records. | | |
| **CA-6 – Security Authorization (Low)** | | |
| **Control**<br>The organization updates the security authorization:<br>- At least every three (3) years;<br>- When substantial changes are made to the system;<br>- When changes in requirements result in the need to process data of a higher sensitivity;<br>- When changes occur to authorizing legislation or federal requirements;<br>- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and<br>- Prior to expiration of a previous security authorization. | | |

**Guidance**

Security authorization is the official management decision, conveyed through the authorization decision document, given by the CMS CIO or his/her designated representative (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to CMS operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of 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 the security risks associated with CMS information system operations. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the CMS CIO and the applicable information system Business Owner with an up-to-date status of the security state of the information system.

To reduce the administrative cost of security reauthorization, the CMS CIO uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. OMB policy requires that federal information systems are reauthorized at least every three years or when there is a significant change to the system.

A significant change to the information system includes a physical, administrative, or technical modification that alters the degree of protection required. Examples include, but are not limited to, changes in operating systems, computer hardware, firmware, operational environment, or system boundaries; new services or applications; or other conditions that potentially impact the system's security posture or authorization status.

| **Applicability:** All | **Reference(s):** FISCAM: SM-2, SM-5; HSPD 7: F(19) | **Related Controls**<br>**Requirement(s):** CA-1, CA-2, CA-4, CA-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-6.1**

**Assessment Objective**

Determine if:

the organization defines in the security plan, explicitly or by reference, the frequency of authorization updates, not to exceed three years;

the organization updates the security authorization:
- at least every three (3) years;
- when substantial 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;
- 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;

a senior organizational official signs and approves the security authorization package.

**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); other relevant documents or records.

**CA-7 – Continuous Monitoring (Low)**

**Control**

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. A configuration management process for the information system and its constituent components;
b. A determination of the security impact of changes to the information system and environment of operation;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
d. Reporting the security state of the information system to appropriate organizational officials within every three hundred sixty-five (365) days.

**Guidance**

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-5; HSPD 7: F(19) | **Related Controls**<br>**Requirement(s):** CA-2, CA-4, CA-5, CA-6, CM-4, SI-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-7.1**

**Assessment Objective**

Determine if:

the organization establishes a continuous monitoring strategy and program;

the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials;

the organization defines organizational officials to whom the security state of the information system should be reported;

the organization implements a continuous monitoring program that includes:
- a configuration management process for the information system and its constituent components;
- a determination of the security impact of changes to the information system and environment of operation;
- ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records.

**CA-7(1) – Enhancement (Low)**

**Control**

The use of independent security assessment agents or teams to monitor security controls is not required. However, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.

**Guidance**

The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's three-year authorization cycle. See supplemental guidance for CA-2, enhancement (1), for further information on assessor independence.

| **Applicability:** All | **Reference(s):** | **Related Controls**<br>**Requirement(s):** AC-9, CA-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: CA-7(1).1**

**Assessment Objective**

Determine if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

| CA-7(2) – Enhancement (Low) | | |
|---|---|---|
| **Control**<br>CMS plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all CMS information systems and information systems that are processing data on behalf of or directly for CMS including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures. | | |
| **Guidance**<br>Examples of vulnerability mitigation procedures are contained in Information Assurance Vulnerability Alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing could also provide evidence of independent validation. See supplemental guidance for CA-2, enhancement (2) for further information on malicious user testing, penetration testing, and other forms of security testing. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** CA-2 |
| **ASSESSMENT PROCEDURE: CA-7(2).1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization defines:<br>- the forms of security testing to be included in planning, scheduling, and security control assessments selecting from in-depth monitoring, malicious user testing, penetration testing, or an organization-defined form of security testing to ensure compliance with all vulnerability mitigation procedures;<br>- the frequency for conducting each form of security testing;<br>- whether the security testing will be announced or unannounced;<br>the organization plans, schedules, and conducts assessments using organization-defined forms of security testing in accordance with the organization-defined frequency and assessment techniques established for each form of testing to ensure compliance with all vulnerability mitigation procedures. | | |

**Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing vulnerability mitigation; 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.

# 5.0CONFIGURATION MANAGEMENT (CM) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CM-1 – Configuration Management Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-1, CP-2, SM-1, SM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CM-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents configuration management policy; | | |

the organization configuration management policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities;

the organization develops and formally documents configuration management procedures;

the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls;

the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities;

the organization reviews/updates the configuration management policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Configuration management policy and procedures; other relevant documents or records.

**CM-2 – Baseline Configuration (Low)**

**Control**

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

**Guidance**

This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of a CMS information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with CMS' enterprise architecture.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|
| **ASSESSMENT PROCEDURE: CM-2.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and documents a baseline configuration of the information system;<br>the organization maintains, under configuration control, a current baseline configuration of the information system.<br>the organization documents deviations from the baseline configuration, in support of mission needs/objectives.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |
| **CM-4 – Security Impact Analysis (Low)** | | |
| **Control**<br>The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system are audited. | | |
| **Guidance**<br>Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-3, CM-3, CM-4, SM-5 | **Related Controls Requirement(s):** CA-7, CM-3 |

**ASSESSMENT PROCEDURE: CM-4.1**

**Assessment Objective**

Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

**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 architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

**CM-6 – Configuration Settings (Low)**

**Control**

The organization:
a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

**Implementation Standard(s)**

1. 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 all security configuration guidelines is as follows:
(a) CMS
(b) DHHS
(c) OMB
(d) NIST
(e) DISA.

**Guidance**

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, AS-3, CM-2, CM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** CM-3, CM-8, SI-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-6.1**

**Assessment Objective**

Determine if:

the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed;

the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;

the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;

the organization implements the security configuration settings;

the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements;

the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

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

**CM-7 – Least Functionality (Low)**

**Control**

The organization configures the information system to provide only essential capabilities and specifically disables, prohibits, or restricts the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.

**Guidance**

Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential CMS operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, 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 server or web server, not both). The functions and services provided by CMS information systems, or individual components of CMS information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-3, CM-3; IRS-1075: 5.6.2.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-7.1**

**Assessment Objective**

Determine if:
the organization defines for the information system prohibited or restricted:
- functions;
- ports;
- protocols;
- services;

the organization configures the information system to provide only essential capabilities;

the organization configures the information system to specifically prohibit or restrict the use of organization-defined:
- functions;
- ports;
- protocols; and/or
- services.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.

**CM-8 – Information System Component Inventory (Low)**

**Control**

The organization develops, documents, and maintains an inventory of information system components that:
a. Accurately reflects the current information system;
b. Is consistent with the authorization boundary of the information system;
c. Is at the level of granularity deemed necessary for tracking and reporting;
d. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and
e. Is available for review and audit by designated organizational officials.

**Guidance**

Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, 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.

| **Applicability:** All | **Reference(s):** FISCAM: CM-2, SM-1; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii) | **Related Controls Requirement(s):** CM-6 |
|---|---|---|

**ASSESSMENT PROCEDURE: CM-8.1**

**Assessment Objective**

Determine if:
the organization defines information deemed necessary to achieve effective property accountability;

the organization develops, documents, and maintains an inventory of information system components that:
- accurately reflects the current information system;
- is consistent with the authorization boundary of the information system;
- is at the level of granularity deemed necessary for tracking and reporting;
- includes organization-defined information deemed necessary to achieve effective property accountability;
- is available for review and audit by designated organizational officials.

**Assessment Methods And Objects**

**Examine:** Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; other relevant documents or records.

# 6.0 CONTINGENCY PLANNING (CP) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **CP-1 – Contingency Planning Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-5, CP-1, CP-3, SM-1, SM-3; HIPAA: 164.308(a)(7)(i), 164.308(a)(7)(ii)(B); IRS-1075: 5.6.2.2#1.1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents contingency planning policy; | | |

the organization contingency planning policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities;

the organization develops and formally documents contingency planning procedures;

the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls;

the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities;

the organization reviews/updates the contingency planning policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy and procedures; other relevant documents or records.

| CP-2 – Contingency Plan (Low) |
|---|
| **Control**<br>The organization:<br>a. Develops a Contingency Plan (CP) for the information system that:<br>- Identifies essential CMS missions and business functions and associated contingency requirements;<br>- Provides recovery objectives, restoration priorities, and metrics;<br>- Addresses contingency roles, responsibilities, assigned individuals with contact information;<br>- Addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure;<br>- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and<br>- Is reviewed and approved by designated officials within the organization;<br>b. Distributes copies of the CP plan to key contingency personnel (identified by name and/or by role) and organizational elements;<br>c. Coordinates contingency planning activities with incident handling activities;<br>d. Reviews the CP for the information system within every three hundred sixty-five (365) days;<br>e. Revises the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing; and<br>f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements. |
| **Guidance**<br>Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for CMS mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Copies of the current CP are stored in a secure location at an alternate site accessible by management and other key personnel. |

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-1, CP-2, CP-3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-2.1**

**Assessment Objective**

Determine if:
the organization develops a contingency plan for the information system that:
- identifies essential missions and business functions and associated contingency requirements;
- provides recovery objectives, restoration priorities, and metrics;
- addresses contingency roles, responsibilities, assigned individuals with contact information;
- addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;
-is reviewed and approved by designated officials within the organization;

the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan;

the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.

**ASSESSMENT PROCEDURE: CP-2.2**

**Assessment Objective**

Determine if:
the organization coordinates contingency planning activities with incident handling activities;

the organization defines the frequency of contingency plan reviews;

the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;

the organization revises 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;

the organization communicates contingency plan changes to the key contingency personnel and organizational elements.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.

**CP-3 – Contingency Training (Low)**

**Control**

The organization trains operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days.

**Guidance**

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 confirmed that appropriate training has been completed.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2; HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-3.1**

**Assessment Objective**

Determine if:

the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is at least annually;

the organization provides refresher training in accordance with organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records.

## CP-4 – Contingency Plan Testing and Exercises (Low)

**Control**

The organization:
a. Tests and/or exercises the contingency plan for the CMS information system within every three hundred sixty-five (365) days using defined tests and exercises, such as the tabletop test in accordance with the current CMS contingency plan procedure to determine the plan's effectiveness and the organization's readiness to execute the plan; and
b. Documents and reviews the contingency plan test/exercise results and initiates reasonable and appropriate corrective actions to close or reduce the impact of contingency plan failures and deficiencies.

**Guidance**

There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on CMS operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-2, CP-4; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-4.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted;

the organization defines in the security plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is at least annually;

the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;

the organization reviews the contingency plan test/exercise results and takes corrective actions.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.

**CP-5 – Contingency Plan Update (Low)**

**Control**

[Withdrawn: Incorporated into CP-2].

**CP-9 – Information System Backup (Low)**

**Control**

The organization:
a. Conducts backups of user-level information contained in the CMS information system in accordance with the frequency specified in Implementation Standard 1;
b. Conducts backups of system-level information contained in the CMS information system in accordance with the frequency specified in Implementation Standard 1;
c. Conducts backups of CMS information system documentation including security-related documentation and other forms of data, including paper records; and
d. Protects the confidentiality and integrity of CMS backup information at the storage location.

**Implementation Standard(s)**

1. Perform backups of user-level and system-level information (including system state information) every month.

**Guidance**

System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control.
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.

| **Applicability:** All | **Reference(s):** FISCAM: AS-5, CP-2; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6 | **Related Controls**<br>**Requirement(s):** MP-4, MP-5 |
|---|---|---|

**ASSESSMENT PROCEDURE: CP-9.1**

**Assessment Objective**

Determine if:
the organization backs up user-level information in accordance with the frequency specified in Implementation Standard 1;

the organization backs up system-level information in accordance with the frequency specified in Implementation Standard 1;

the organization backs up information system documentation (including security-related information and other forms of data).

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; backup storage location(s); information system backup logs or records; other relevant documents or records.

**ASSESSMENT PROCEDURE: CP-9.2**

**Assessment Objective**

Determine if the organization protects the confidentiality and integrity of backup information at the storage location.

**Assessment Methods And Objects**

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; information system configuration settings and associated documentation; backup storage location(s); other relevant documents or records.

**CP-9(4) – Enhancement (Low)**

**Control**

[Withdrawn: Incorporated into CP-9].

| CP-10 – Information System Recovery and Reconstitution (Low) | | |
|---|---|---|
| **Control**<br>The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.<br>**Implementation Standard(s)**<br>1. Secure information system recovery and reconstitution includes, but not limited to:<br>(a) Reset all system parameters (either default or organization-established),<br>(b) Reinstall patches,<br>(c) Reestablish configuration settings,<br>(d) Reinstall application and system software, and<br>(e) Fully test the system. | | |
| **Guidance**<br>Recovery is executing information system contingency plan activities to restore essential CMS missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on CMS priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. | | |
| **Applicability:** All | **Reference(s):** FISCAM: CP-2, CP-3, CP-4; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: CP-10.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure; | | |

the organization provides for the recovery of the information system after a failure or other contingency in a trusted, secure, and verifiable manner.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**CP-10(1) – Enhancement (Low)**

**Control**

[Withdrawn: Incorporated into CP-4].

# 7.0 IDENTIFICATION AND AUTHENTICATION (IA) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **IA-1 – Identification and Authentication Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.3.1#1.1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents identification and authentication policy; | | |

the organization identification and authentication policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities;

the organization develops and formally documents identification and authentication procedures;

the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls;

the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities;

the organization reviews/updates the identification and authentication policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy and procedures; other relevant documents or records.

**IA-2 – Identification and Authentication (Organizational Users) (Low)**

**Control**

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

**Implementation Standard(s)**

1. Require the use of system and/or network authenticators and unique user identifiers.
2. Help desk support requires user identification for any transaction that has information security implications.

**Guidance**

Organizational users (i.e., CMS information system users) include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to CMS information systems is defined as either local or network. Local access is any access to a CMS information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to a CMS information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.

The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 5.6.3.1#1.2, 5.6.3.3#2.3 | **Related Controls Requirement(s):** AC-14, AC-17, MA-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2.1**

**Assessment Objective**

Determine if:

the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**IA-2(1) – Enhancement (Low)**

**Control**

The information system uses multifactor authentication for network access to privileged accounts.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-2(1).1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for network access to privileged accounts.

**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; other relevant documents or records.

| IA-4 – Identifier Management (Low) | | |
|---|---|---|
| **Control**<br>The organization manages CMS information system identifiers for users and devices by:<br>a. Receiving authorization from a designated organizational official to assign a user or device identifier;<br>b. Selecting an identifier that uniquely identifies an individual or device;<br>c. Assigning the user identifier to the intended party or the device identifier to the intended device;<br>d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired; and<br>e. Disabling the user identifier after the time period of inactivity specified in Implementation Standard 1 and deleting disabled accounts during the annual re-certification process.<br>**Implementation Standard(s)**<br>1. Disable user identifiers after three hundred sixty-five (365) days of inactivity. | | |
| **Guidance**<br>Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system).<br>Reviews and validation of system users' accounts are conducted to ensure the continued need for access to a system. Identifier management is applicable to shared information system accounts (i.e., guest and anonymous). | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3, AC-4, AS-2; IRS-1075: 5.6.3.1#2 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: IA-4.1**

**Assessment Objective**

Determine if:
the organization manages information system identifiers for users and devices by:
- receiving authorization from a designated organizational official to assign a user or device identifier;
- selecting an identifier that uniquely identifies an individual or device;
- assigning the user identifier to the intended party or the device identifier to the intended device;
- preventing reuse of user or device identifiers for the organization-defined time period;
- disabling the user identifier after the organization-defined time period of inactivity;

the organization defines in the security plan, explicitly or by reference, the time period of inactivity after which a user identifier is to be disabled.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records.

**IA-5 – Authenticator Management (Low)**

**Control**

The organization manages CMS information system authenticators for users and devices by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/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 upon information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
g. Changing/refreshing password authenticators as defined in IA-5(1);
h. Protecting authenticator content from unauthorized disclosure and modification; and
i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

**Guidance**

User 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). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The CMS information system supports user authenticator management by security 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 verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-2; IRS-1075: 5.6.3.1#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-5.1**

**Assessment Objective**

Determine if:
the organization defines the time period (by authenticator type) for changing/refreshing authenticators;

the organization manages information system authenticators for users and devices by:
- verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- establishing initial authenticator content for authenticators defined by the organization;
- ensuring that authenticators have sufficient strength of mechanism for their intended use;
- establishing and implementing administrative procedures for initial authenticator distribution;
- establishing and implementing administrative procedures for lost/compromised or damaged authenticators;
- establishing and implementing administrative procedures for revoking authenticators;
- changing default content of authenticators upon information system installation;
- establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);
- changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;
- protecting authenticator content from unauthorized disclosure and modification;
- requiring users to take, and having devices implement, specific measures to safeguard authenticators.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

## IA-5(1) – Enhancement (Low)

**Control**

The CMS information system, for password-based authentication:
(a) Automatically forces users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days;
(b) Prohibits the use of dictionary names or words;
(c) Enforces minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lower-case letters, and numbers) and/or special characters;
(d) Enforces at least a minimum of four (4) changed characters when new passwords are created;
(e) Encrypts passwords in storage and in transmission;
(f) Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum; and
(g) Prohibits password reuse for one (1) generation prior to reuse.

**Guidance**

This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does not apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-5(1).1**

**Assessment Objective**

Determine if the information system, for password-based authentication:
- enforces the minimum password complexity standards that meet the organization-defined requirements;
- enforces the organization-defined minimum number of characters that must be changed when new passwords are created;
- encrypts passwords in storage and in transmission;
- enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters;
- prohibits password reuse for the organization-defined number of generations.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

## IA-6 – Authenticator Feedback (Low)

**Control**

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

**Guidance**

The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.

| **Applicability:** All | **Reference(s):** FISCAM: AC-2; IRS-1075: 5.6.3.1#1.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-6.1**

**Assessment Objective**

Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**IA-7 – Cryptographic Module Authentication (Low)**

**Control**

The information system uses 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IA-7.1**

**Assessment Objective**

Determine if the information system uses 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.

**Assessment Methods And Objects**

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

| IA-8 – Identification and Authentication (Non-Organizational Users) (Low) | | |
|---|---|---|
| **Control**<br>The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). | | |
| **Guidance**<br>Non-organizational users include all CMS information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with 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). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered 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 to CMS operations, CMS assets, individuals, other organizations, and the Nation. Identification and authentication requirements for CMS information system access by organizational users are described in IA-2. If E-Authentication is used, refer to ARS Appendix D: E-authentication Standard. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IA-8.1** | | |
| **Assessment Objective**<br>Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).<br>**Assessment Methods And Objects**<br>**Examine:** Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records. | | |

# 8.0 INCIDENT RESPONSE (IR) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **IR-1 – Incident Response Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-1, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: IR-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents incident response policy; | | |

the organization incident response policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities;

the organization develops and formally documents incident response procedures;

the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls;

the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities;

the organization reviews/updates the incident response policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Incident response policy and procedures; other relevant documents or records.

**IR-2 – Incident Response Training (Low)**

**Control**

The organization:
a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and
b. Provides refresher training within every three hundred sixty-five (365) days.

**Guidance**

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Incident response training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. 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 basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
(4) CIOs, IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) 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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.2.6#2.1-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-2.1**

**Assessment Objective**

Determine if:
the organization identifies personnel with incident response roles and responsibilities with respect to the information system;

the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;

incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually;

the organization provides refresher incident response training in accordance with organization-defined frequency.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records.

**IR-4 – Incident Handling (Low)**

**Control**

The organization:
a. Implements an incident handling capability using CMS Information Security Incident Handling and Breach Notification Procedures;
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 Standard(s)**

1. Document relevant information related to a security incident according to CMS Information Security Incident Handling and Breach Notification Procedures.
2. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.
3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure.

**Guidance**

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3 | **Related Controls Requirement(s):** AU-6, PE-6, SI-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-4.1**

**Assessment Objective**

Determine if:
the organization implements an incident handling capability for security incidents that includes:
- preparation;
- detection and analysis;
- containment;
- eradication;
- recovery;

the organization coordinates incident handling activities with contingency planning activities;

the organization incorporates lessons learned from ongoing incident handling activities into:
- incident response procedures;
- training;
- testing/exercises;

the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.

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; other relevant documents or records.

**IR-5 – Incident Monitoring (Low)**

**Control**

The organization tracks and documents information system security incidents.

**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.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, SM-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#2.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-5.1**

**Assessment Objective**

Determine if the organization tracks and documents information system security incidents.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; other relevant documents or records.

**IR-6 – Incident Reporting (Low)**

**Control**

The organization:
a. Requires personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current CMS Information Security Incident Handling and Breach Analysis/Notification Procedure; and
b. Reports security incident information to designated authorities.

**Guidance**

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. CMS requires that events and confirmed security incidents must be reported to the CMS IT Service Desk in accordance with established procedures.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-6.1**

**Assessment Objective**

Determine if:
the organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current CMS Information Security Incident Handling and Breach Analysis/Notification Procedure;

the organization reports security incident information to designated authorities.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records.

**IR-7 – Incident Response Assistance (Low)**

**Control**

The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

**Guidance**

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. The CMS IT Service Desk is available to offer advice to users of a CMS information system.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-7.1**

**Assessment Objective**

Determine if:
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;

the incident response support resource is an integral part of the organization's incident response capability.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

**IR-8 – Incident Response Plan (Low)**

**Control**

The organization:
a. Develops an incident response plan that:
- Provides the organization with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall organization;
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the organization.
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved by designated officials within the organization;
b. Distributes copies of the incident response plan to incident response personnel and organizational elements;
c. Reviews the incident response plan within every three hundred sixty-five (365) days;
d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
e. Communicates incident response plan changes to incident response personnel and organizational elements.

**Guidance**

It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: IR-8.1**

**Assessment Objective**

Determine if the organization develops an incident response plan that:
- provides the organization with a roadmap for implementing its incident response capability;
- describes the structure and organization of the incident response capability;
- provides a high-level approach for how the incident response capability fits into the overall organization;
- meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- defines reportable incidents;
- provides metrics for measuring the incident response capability within the organization;
- defines the resources and management support needed to effectively maintain and mature an incident response capability;
- is reviewed and approved by designated officials within the organization.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

**ASSESSMENT PROCEDURE: IR-8.2**

**Assessment Objective**

Determine if:
the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;

the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan;

the organization reviews the incident response plan in accordance with the organization-defined frequency;

the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

# 9.0 MAINTENANCE (MA) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **MA-1 – System Maintenance Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, CM-5, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system maintenance policy; | | |

the organization system maintenance policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities;

the organization develops and formally documents system maintenance procedures;

the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls;

the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities;

the organization reviews/updates the information system maintenance policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy and procedures; other relevant documents or records.

## MA-2 – Controlled Maintenance (Low)

**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. Controls 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 a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

**Guidance**

The control is intended to address the information security aspects of the organization's CMS information system maintenance program. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

| **Applicability:** All; Optional for SS | **Reference(s):** FISCAM: AC-6, CP-2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-2.1**

**Assessment Objective**

Determine if:
the organization 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;

the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

**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; other relevant documents or records.

| MA-4 – Non-Local Maintenance (Low) | | |
|---|---|---|
| **Control**<br>The organization prohibits non-local CMS system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:<br>a. Monitors and controls non-local maintenance and diagnostic activities;<br>b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;<br>c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;<br>d. Maintains records for non-local maintenance and diagnostic activities; and<br>e. Terminates all sessions and network connections when non-local maintenance is completed.<br>**Implementation Standard(s)**<br>1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service. | | |
| **Guidance**<br>Non-local 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. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. 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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4, SM-7; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3 | **Related Controls Requirement(s):** IA-2, MP-6 |
| **ASSESSMENT PROCEDURE: MA-4.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization prohibits non-local CMS system maintenance unless explicitly authorized, in writing, by the CIO; | | |

if authorized, the organization monitors and controls non-local maintenance and diagnostic activities;

if authorized, the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools;

if authorized, the organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;

if authorized, the organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;

if authorized, the organization terminates all sessions and network connections when non-local maintenance is completed.

if authorized, the organization maintains records for non-local maintenance and diagnostic activities;

if authorized, the organization (or information system in certain cases) terminates all sessions and network connections when non-local maintenance or diagnostics is completed.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

## MA-5 – Maintenance Personnel (Low)

**Control**

The organization:
a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and
b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

**Guidance**

Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2, SM-7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MA-5.1**

**Assessment Objective**

Determine if:
the organization establishes a process for maintenance personnel authorization;

the organization maintains a current list of authorized maintenance organizations or personnel;

personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance.

**Assessment Methods And Objects**

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

# *10.0* MEDIA PROTECTION (MP) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **MP-1 – Media Protection Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SM-1, SM-3; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: MP-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents media protection policy; | | |

the organization media protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities;

the organization develops and formally documents media protection procedures;

the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls;

the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities.

the organization reviews/updates the media protection policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Media protection policy and procedures; other relevant documents or records.

**MP-2 – Media Access (Low)**

**Control**

The organization restricts access to CMS sensitive digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.

**Guidance**

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4, AC-6, BP-3; HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: MP-2.1**

**Assessment Objective**

Determine if:
the organization defines:
- digital and non-digital media requiring restricted access;
- individuals authorized to access the media;
- security measures taken to restrict access;

the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures.

**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; other relevant documents or records.

| MP-6 – Media Sanitization (Low) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and<br>b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.<br>**Implementation Standard(s)**<br>1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures. | | |
| **Guidance**<br>This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of sensitive information to unauthorized individuals when such media is reused or released for disposal. The organization uses its discretion on the employment of 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 CMS or individuals if released for reuse or disposal. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-1075: 4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2 | **Related Controls**<br>**Requirement(s):** MA-4 |
| **ASSESSMENT PROCEDURE: MP-6.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization sanitizes information system media both digital and non-digital prior to:<br>- disposal;<br>- release out of organizational control; or<br>- release for reuse;<br>the organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. | | |

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records.

# 11.0 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PE-1 – Physical and Environmental Protection Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-2, CP-2, SM-1, SM-3; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents physical and environmental protection policy; | | |

the organization physical and environmental protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities;

the organization develops and formally documents physical and environmental protection procedures;

the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls;

the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities;

the organization reviews/updates the physical and environmental protection policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy and procedures; other relevant documents or records.

## PE-2 – Physical Access Authorizations (Low)

**Control**

The organization:
a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
b. Issues authorization credentials;
c. Reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.

**Implementation Standard(s)**

1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every three hundred sixty-five (365) days.

| **Guidance**<br>Authorization credentials include, for example, badges, identification cards, and smart cards. | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-2.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization identifies areas within the facility that are publicly accessible;<br>the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);<br>the organization issues authorization credentials (e.g., badges, identification cards, smart cards).<br>the organization reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |

| PE-3 – Physical Access Control (Low) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);<br>b. Verifies individual access authorizations before granting access to the facility;<br>c. Controls entry to the facility containing the information system using physical access devices and/or guards;<br>d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;<br>e. Controls access authorization lists to secure areas;<br>f. Secures keys, combinations, and other physical access devices;<br>g. Inventories physical access devices within every three hundred sixty-five (365) days; and<br>h. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.<br>**Implementation Standard(s)**<br>1. Control data center/facility access by use of door and window locks.<br>2. Store and operate servers in physically secure environments protected from unauthorized access. | | |
| **Guidance**<br>The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) a CMS information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SD-1, SM-4; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: PE-3.1**

**Assessment Objective**

Determine if:
the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

the organization verifies individual access authorizations before granting access to the facility;

the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;

the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

the organization secures keys, combinations, and other physical access devices;

the organization inventories physical access devices within every three hundred sixty-five (365) days;

the organization changes combinations and keys periodically; and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PE-6 – Monitoring Physical Access (Low)**

**Control**

The organization:
a. Monitors physical access to the information system to detect and respond to physical security incidents;
b. Reviews physical access logs in accordance with the frequency specified in Implementation Standard 1; and
c. Coordinates results of reviews and investigations with the organization's incident response capability.

**Implementation Standard(s)**

1. Review physical access logs every at least once every three (3) months.

**Guidance**

Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AC-6, SM-5 | **Related Controls Requirement(s):** IR-4 |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-6.1**

**Assessment Objective**

Determine if:
the organization monitors physical access to the information system to detect and respond to physical security incidents;

the organization reviews physical access logs in accordance with the organization-defined frequency;

the organization coordinates results of reviews and investigations with the organization's incident response capability.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PE-7 – Visitor Control (Low)**

**Control**

The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

**Guidance**

Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6; HIPAA: 164.310(a)(2)(iii) | **Related Controls Requirement(s):** |
|---|---|---|

| ASSESSMENT PROCEDURE: PE-7.1 | | |
|---|---|---|
| **Assessment Objective**<br>Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.<br>**Assessment Methods And Objects**<br>**Examine:** Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records. | | |
| **PE-8 – Access Records (Low)** | | |
| **Control**<br>The organization:<br>a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and<br>b. Closes and reviews visitor access records monthly. | | |
| **Guidance**<br>Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-8.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);<br>the organization reviews the visitor access records in accordance with the organization-defined frequency.<br>**Assessment Methods And Objects**<br>**Examine:** Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; other relevant documents or records. | | |

| PE-12 – Emergency Lighting (Low) | | |
|---|---|---|
| **Control**<br>The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. | | |
| **Guidance**<br>This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PE-12.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption;<br>the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility;<br>the organization maintains the automatic emergency lighting for the information system. | | |
| **Assessment Methods And Objects**<br>**Examine:** Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records. | | |
| **PE-13 – Fire Protection (Low)** | | |
| **Control**<br>The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. | | |

**Guidance**

Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-13.1**

**Assessment Objective**

Determine if:
the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source;

the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

**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; other relevant documents or records.

## PE-14 – Temperature and Humidity Controls (Low)

**Control**

The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and
b. Monitors temperature and humidity levels.

**Implementation Standard(s)**

1. Evaluate the level of alert and follow prescribed guidelines for that alert level.

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-14.1**

**Assessment Objective**

Determine if:
the organization defines the acceptable temperature and humidity levels within the facility where the information system resides;

the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels;

the organization defines the frequency to monitor temperature and humidity levels;

the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PE-15 – Water Damage Protection (Low)**

**Control**

The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

**Guidance**

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, CP-2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-15.1**

**Assessment Objective**

Determine if:
the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly;

key personnel within the organization have knowledge of the master water shutoff values.

**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; other relevant documents or records.

**PE-16 – Delivery and Removal (Low)**

**Control**

The organization authorizes, monitors, and controls the flow of CMS information system-related components entering and exiting the facility and maintains records of those items.

**Guidance**

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PE-16.1**

**Assessment Objective**

Determine if:
the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility;

the organization maintains records of information system components entering and exiting the facility.

**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; other relevant documents or records.

# 12.0 PLANNING (PL) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PL-1 – Security Planning Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PL-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents security planning policy; | | |

the organization security planning policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities;

the organization develops and formally documents security planning procedures;

the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls;

the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities;

the organization reviews/updates the security planning policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Security planning policy and procedures; other relevant documents or records.

| PL-2 – System Security Plan (SSP) (Low) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Develops a security plan for the information system that:<br>- Is consistent with the CMS System Security Plan (SSP) Procedure;<br>- Is consistent with the organization's enterprise architecture;<br>- Explicitly defines the authorization boundary for the system;<br>- Describes the operational context of the information system in terms of missions and business processes;<br>- Provides the security categorization of the information system including supporting rationale;<br>- Describes the operational environment for the information system;<br>- Describes relationships with or connections to other information systems;<br>- Provides an overview of the security requirements for the system;<br>- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and<br>- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;<br>b. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and<br>c. Updates the plan, minimally every three (3) years, to address current conditions or whenever:<br>- There are significant changes to the information system/environment of operation that affect security;<br>- Problems are identified during plan implementation or security control assessments:<br>- When the data sensitivity level increases;<br>- After a serious security violation due to changes in the threat environment; or<br>- Before the previous security authorization expires. | | |
| **Guidance**<br>The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to CMS operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended.<br>All CMS information systems and major applications are covered by an SSP, which is compliant with current CMS SSP Procedures. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, CP-1, CP-2, SM-1; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: PL-2.1**

**Assessment Objective**

Determine if:
the organization develops a security plan for the information system that:
- is consistent with the organization's enterprise architecture;
- explicitly defines the authorization boundary for the system;
- describes the operational context of the information system in terms of mission and business processes;
- provides the security categorization of the information system including supporting rationale;
- describes the operational environment for the information system;
- describes relationships with or connections to other information systems;
- provides an overview of the security requirements for the system;
- describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions;
- is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

the organization defines the frequency of security plan reviews;

the organization reviews the security plan in accordance with the organization-defined frequency, minimally every three (3) years;

the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

**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; other relevant documents or records.

**PL-3 – System Security Plan Update (Low)**

**Control**

[Withdrawn: Incorporated into PL-2].

| PL-4 – Rules of Behavior (ROB) (Low) | | |
|---|---|---|
| **Control**<br>The organization:<br>a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information, information system, and network use; and<br>b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. | | |
| **Guidance**<br>The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior.<br>ROBs are aligned with DHHS requirements posted at http://hhs.gov/ocio/policy/2008-0001.003s.html, and made readily available. | | |
| **Applicability:** All | **Reference(s):** FISCAM: CP-2, SM-4; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.5 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PL-4.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;<br>the organization makes the rules available to all information system users;<br>the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. | | |
| **Assessment Methods And Objects**<br>**Examine:** Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records. | | |

| PL-5 – Privacy Impact Assessment (PIA) (Low) | | |
|---|---|---|
| **Control**<br>The organization conducts a Privacy Impact Assessment (PIA) on the information system in accordance with OMB policy. | | |
| **Applicability:** All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC | **Reference(s):** FISCAM: SM-5; HSPD 7: J(35) | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PL-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization conducts a privacy impact assessment on the information system;<br>the privacy impact assessment is in accordance with OMB policy.<br>**Assessment Methods And Objects**<br>**Examine:** Security planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records. | | |

# 13.0 PERSONNEL SECURITY (PS) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **PS-1 – Personnel Security Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SD-2, SM-1, SM-3, SM-4; IRS-1075: 5.6.2.1#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PS-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents personnel security policy; | | |

the organization personnel security policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities;

the organization develops and formally documents personnel security procedures;

the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls;

the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities;

the organization reviews/updates the personnel security policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Personnel security policy and procedures, other relevant documents or records.

**PS-2 – Position Categorization (Low)**

**Control**

The organization:
a. Assigns a criticality/sensitivity risk designation to all positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and revises position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.

**Guidance**

Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).

| **Applicability:** All | **Reference(s):** FISCAM: SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-2.1**

**Assessment Objective**

Determine if:
the organization assigns a risk designations to all positions within the organization;

the organization establishes a screening criteria for individuals filling organizational positions;

the organization defines in the security plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions;

the organization reviews/revises position risk designations within every three hundred sixty-five (365) days.

**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; other relevant documents or records.

**PS-3 – Personnel Screening (Low)**

**Control**

The organization:
a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position.

**Implementation Standard(s)**

1. Perform criminal history check for all persons prior to employment.
2. Require appropriate personnel to obtain and hold a low-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

**Guidance**

Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. For prospective employees, references background checks are performed before issuance of a User ID. Security agreements are required for employees and contractors assigned to work with mission critical information.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, SM-4, SM-7; IRS-1075: 5.6.2.1#1.4 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-3.1**

**Assessment Objective**

Determine if:
the organization screens individuals prior to authorizing access to the information system;

the organization rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position;

the personnel screening is consistent with 5 CFR 731.106, OPM policy, regulations, and guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records.

**PS-4 – Personnel Termination (Low)**

**Control**

The organization, upon termination of individual employment:
a. Revokes system and physical access immediately following employee termination;
b. Conducts exit interviews;
c. Retrieves all security-related CMS information system-related property;
d. Retains access to CMS information and information systems formerly controlled by terminated individual; and
e. Immediately escorts employees terminated for cause out of the organization.

**Implementation Standard(s)**

1. System access must be revoked immediately following employee termination.

**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 individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all CMS information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and nonavailability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause. Appropriate personnel have access to official records created by the terminated employee that are stored on CMS information systems.

| **Applicability:** All | **Reference(s):** FISCAM: SM-4; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: 5.6.2.1#1.5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-4.1**

**Assessment Objective**

Determine if:

the organization terminates information system access upon termination of individual employment;

the organization conducts exit interviews of terminated personnel;

the organization retrieves all security-related CMS information system-related property from terminated personnel;

the organization, upon termination of individual employment, retrieves all security-related CMS information system-related property;

the organization, upon termination of individual employment, retains access to CMS information and information systems formerly controlled by terminated individual;

the organization, upon termination of individual employment, immediately escorts employees terminated for cause out of the organization.

the organization meets all the requirements specified in the applicable implementation standard(s).

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.

| PS-5 – Personnel Transfer (Low) | | |
|---|---|---|
| **Control**<br>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 the following transfer or reassignment actions during the formal transfer process:<br>a. Re-issuing appropriate CMS information system-related property (e.g., keys, identification cards, building passes);<br>b. Notification to security management;<br>c. Closing obsolete accounts and establishing new accounts; and<br>d. Revocation of all system access privileges (if applicable). | | |
| **Guidance**<br>This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts. | | |
| **Applicability:** All | **Reference(s):** FISCAM: SM-4; IRS-1075: 5.6.2.1#1.6 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: PS-5.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization;<br>the organization defines the transfer or reassignment actions and the time period within which the actions must occur following formal transfer or reassignment;<br>the organization initiates the organization-defined transfer or reassignment actions within an organization-defined time period following formal transfer or reassignment. | | |

**Assessment Methods And Objects**

**Examine:** Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

**PS-6 – Access Agreements (Low)**

**Control**

The organization:
a. Ensures that individuals requiring access to CMS information or information systems sign appropriate access agreements prior to being granted access; and
b. Reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended.

**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 the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-6.1**

**Assessment Objective**

Determine if:
the organization identifies appropriate access agreements for individuals requiring access to CMS information and information systems;

individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access;

the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates for access agreements;

the organization reviews/updates the access agreements in accordance with the organization-defined frequency.

**Assessment Methods And Objects**

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

## PS-7 – Third-Party Personnel Security (Low)

**Control**

The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Documents personnel security requirements; and
c. Monitors provider compliance.

**Implementation Standard(s)**

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 CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies and standards.

**Guidance**

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. Security requirements include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements.

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, SD-1, SM-4, SM-7; IRS-1075: 5.6.2.1#1.8 | **Related Controls Requirement(s):** |
|---|---|---|

### ASSESSMENT PROCEDURE: PS-7.1

**Assessment Objective**

Determine if:
the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers;

the organization documents personnel security requirements for third-party providers;

the organization monitors third-party provider compliance with personnel security requirements.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**PS-8 – Personnel Sanctions (Low)**

**Control**

The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

**Guidance**

The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, SD-2, SM-4; HIPAA: 164.308(a)(1)(ii)(C) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: PS-8.1**

**Assessment Objective**

Determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

**Assessment Methods And Objects**

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

# 14.0 RISK ASSESSMENT (RA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **RA-1 – Risk Assessment Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-2, SM-3; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075: 5.6.1.1#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: RA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents risk assessment policy; | | |

the organization risk assessment policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities;

the organization develops and formally documents risk assessment procedures;

the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls;

the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities;

the organization reviews/updates the risk assessment policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy and procedures; other relevant documents or records.

**RA-2 – Security Categorization (Low)**

**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 designated representative.

**Guidance**

A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to CMS operations, CMS assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the CMS CIO, CISO, Business Owner, senior information security officer, and information owners/stewards. The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted.
All CMS information systems categorized as High or Moderate are considered sensitive or to contain sensitive information. All CMS information systems categorized as Low are considered non-sensitive or to 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.

| **Applicability:** All | **Reference(s):** FISCAM: CP-1, SM-2; HSPD 7: D(8); IRS-1075: 4.1#2 | **Related Controls Requirement(s):** MP-4, SC-7 |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-2.1**

**Assessment Objective**

Determine if:
the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

the organization documents the security categorization results (including supporting rationale) in the security plan for the information system;

the CMS authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

**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; other relevant documents or records.

| RA-3 – Risk Assessment (Low) |
|---|
| **Control**<br>The organization:<br>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;<br>b. Documents risk assessment results in accordance with the CMS Information Security (IS) Risk Assessment (RA) Procedures;<br>c. Reviews risk assessment results within every three hundred sixty-five (365) days; and<br>d. Updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. |
| **Guidance**<br>A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to CMS operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to CMS operations, CMS assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing CMS information systems, outsourcing entities).<br>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. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems.<br>Risk assessments can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the baselines with additional security controls or control enhancements. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-6, AS-1, AS-5, CP-1, CP-2, SM-2; HIPAA: 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3, 6.3.3#2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-3.1**

**Assessment Objective**

Determine if:
the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:
- access;
- use;
- disclosure;
- disruption;
- modification; or
- destruction;

the organization documents risk assessment results in accordance with the CMS IS RA Procedures;

the organization reviews risk assessment results within every three hundred sixty-five (365) days;

the organization updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records.

**RA-4 – Risk Assessment Update (Low)**

**Control**

[Withdrawn: Incorporated into RA-3].

| RA-5 – Vulnerability Scanning (Low) |
| --- |
| **Control**<br>The organization:<br>a. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:<br>- Enumerating platforms, software flaws, and improper configurations;<br>- Formatting and making transparent, checklists and test procedures; and<br>- Measuring vulnerability impact;<br>b. Analyzes vulnerability scan reports and results from security control assessments;<br>c. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and<br>d. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).<br>**Implementation Standard(s)**<br>1. Scans for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported.<br>2. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with CMS IS procedures. |
| **Guidance**<br>The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan. |

| **Applicability:** All | **Reference(s):** FISCAM: CM-5, SM-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: RA-5.1**

**Assessment Objective**

Determine if:
the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:
- enumerating platforms, software flaws, and improper configurations;
- formatting/and making transparent checklists and test procedures;
- measuring vulnerability impact;

the organization analyzes vulnerability scan reports and results from security control assessments;

the organization remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk;

the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.

# 15.0 SYSTEM AND SERVICES ACQUISITION (SA) – *MANAGEMENT*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **SA-1 – System and Services Acquisition Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.1.3#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SA-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system services and acquisition policy; | | |

the organization system services and acquisition policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system services and acquisition policy to elements within the organization having associated system services and acquisition roles and responsibilities;

the organization develops and formally documents system services and acquisition procedures;

the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls;

the organization disseminates formal documented system services and acquisition procedures to elements within the organization having associated system services and acquisition roles and responsibilities;

the organization reviews/updates the system services and acquisition policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** System and services acquisition policy and procedures; other relevant documents or records.

## SA-2 – Allocation of Resources (Low)

**Control**

The organization:
a. Includes a determination of information security requirements for the information system in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system 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' programming and budgeting documentation for the implementation and management of information systems security.

| **Applicability:** All | **Reference(s):** FISCAM: CM-3, IN-2, SD-1, SM-1 | **Related Controls Requirement(s):** |
|---|---|---|

| **ASSESSMENT PROCEDURE: SA-2.1** | | |
|---|---|---|
| **Assessment Objective**<br>Determine if:<br>the organization includes a determination of the information security requirements for the information system in mission/business process planning;<br>the organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process;<br>the organization establishes a discrete line item for information security in organizational programming and budgeting documentation;<br>the organization establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security.<br>**Assessment Methods And Objects**<br>**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. | | |
| **SA-3 – Life Cycle Support (Low)** | | |
| **Control**<br>The organization:<br>a. Manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS Integrated IT Investment & System Life Cycle Framework (ILC);<br>b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and<br>c. Identifies individuals having information system security roles and responsibilities. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AS-3, AS-5, BP-1, BP-2, BP-3, BP-4, CM-1, CM-3, CP-3, DA-1, IN-1 | **Related Controls Requirement(s):** |

**ASSESSMENT PROCEDURE: SA-3.1**

**Assessment Objective**

Determine if:
the organization manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS Integrated IT Investment & System Life Cycle Framework (ILC);

the organization defines and documents information system security roles and responsibilities throughout the system development life cycle;

the organization identifies individuals having information system security roles and responsibilities.

**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.

**SA-4 – Acquisitions (Low)**

**Control**

The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
a. Security functional requirements/specifications;
b. Security-related documentation requirements; and
c. Developmental and evaluation-related assurance requirements.

**Implementation Standard(s)**

1. Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

**Guidance**

The acquisition documents for CMS information systems, CMS information system components, and CMS information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.

Solicitation Documents:

Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required:

- Security capabilities;
- Design and development processes;
- Test and evaluation procedures; and
- Documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

Use of Evaluated and Validated Products:

For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources:

1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-3, SM-7 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-4.1**

**Assessment Objective**

Determine if:
the organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
- security functional requirements/specifications;
- security-related documentation requirements;
- developmental and evaluation-related assurance requirements.

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 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.

**SA-5 – Information System Documentation (Low)**

**Control**

The organization:
a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
- Secure configuration, installation, and operation of the information system;
- Effective use and maintenance of security features/functions; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and

b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
- User-accessible security features/functions and how to effectively use those security features/functions;
- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
- User responsibilities in maintaining the security of the information and information system; and

c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

**Implementation Standard(s)**

1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.
2. Maintain an updated list of related system operations and security documentation.
3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation.

**Guidance**

The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, AS-2, AS-3, AS-4, AS-5, BP-1, BP-2, BP-3, BP-4, CM-2, CM-3, CP-2, DA-1, IN-1, IN-2, SD-1, SD-2; IRS-1075: 5.6.1.3#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-5.1**

**Assessment Objective**

Determine if:
the organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
- secure configuration, installation, and operation of the information system;
- effective use and maintenance of the security features/functions;
- known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

the organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
- user-accessible security features/functions and how to effectively use those security features/functions;
- methods for user interaction with the information system, which enables individuals to use the system in a more secure manner;
- user responsibilities in maintaining the security of the information and information system;

the organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

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 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.

**ASSESSMENT PROCEDURE: SA-5.FIS-1**

**Assessment Objective**

Determine if:
the organization develops information system documentation for operating the system that includes:
- operational instructions and
- appropriate end user control, balancing, and verification features and procedures.

the organization disseminates information system documentation to appropriate elements within the organization;

responsible parties within the organization periodically review information system documentation;

the organization updates information system documentation when organizational review indicates updates are required or changes are made to the system.

**Assessment Methods And Objects**

**Examine:** Information system documentation; other relevant documents or records.

**SA-6 – Software Usage Restrictions (Low)**

**Control**

The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

**Guidance**

Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

| **Applicability:** All | **Reference(s):** FISCAM: CM-3, CM-5; IRS-1075: 4.7.3#1.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-6.1**

**Assessment Objective**

Determine if:
the organization uses software and associated documentation in accordance with contract agreements and copyright laws;

the organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution;

the organization 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.

**Assessment Methods And Objects**

**Examine:** System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records.

**SA-7 – User-Installed Software (Low)**

**Control**

The organization prohibits users from downloading or installing software, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, explicit rules govern the installation of software by users.

**Implementation Standard(s)**

1. If user installed software is authorized, ensure that business rules and technical controls enforce the documented authorizations and prohibitions.

**Guidance**

If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect).

| **Applicability:** All | **Reference(s):** FISCAM: CM-3, CM-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-7.1**

**Assessment Objective**

Determine if:
the organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users;

the organization (or information system) enforces explicit rules governing the installation of software by users.

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 user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records.

**SA-9 – External Information System Services (Low)**

**Control**

The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Monitors security control compliance by external service providers.
d. Prohibits service providers from outsourcing any system function outside the U.S. or its territories.

**Guidance**

An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization 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 to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

| **Applicability:** All | **Reference(s):** FISCAM: AS-1, SM-7; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4 | **Related Controls Requirement(s):** CA-3 |
|---|---|---|

**ASSESSMENT PROCEDURE: SA-9.1**

**Assessment Objective**

Determine if:

the organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services;

the organization monitors security control compliance by external service providers.

the organization prohibits service providers from outsourcing any system function outside the U.S. or its territories.

**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.

# 16.0 SYSTEM AND COMMUNICATIONS PROTECTION (SC) – *TECHNICAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **SC-1 – System and Communications Protection Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, CM-5, SM-1, SM-3; IRS-1075: 5.6.3.4#1, 5.6.3.4#2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system and communications protection policy; | | |

the organization system and communications protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities;

the organization develops and formally documents system and communications protection procedures;

the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls;

the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities;

the organization reviews/updates the system and communications protection policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** System and communications protection policy and procedures; other relevant documents or records.

**SC-5 – Denial of Service Protection (Low)**

**Control**

The information system protects against or limits the effects of the following types of denial of service attacks defined on the following sites or in the following documents:
- SANS Organization www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and
- NIST CVE List http://checklists.nist.gov/home.cfm.

**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 devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-5.1**

**Assessment Objective**

Determine if:
the organization defines in the security plan, explicitly or by reference, the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system;

the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.

**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.

**SC-7 – Boundary Protection (Low)**

**Control**

The information system:
a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
b. Connects to external networks or information systems only through managed interfaces consisting of automated boundary protection devices arranged in accordance with an organizational security architecture.

**Implementation Standard(s)**

1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
2. Although not required, it is recommended that stateful inspection hardware and software is utilized.

**Guidance**

Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected sub-network commonly referred to as a demilitarized zone or DMZ).

The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. When this situation occurs, the organization implements appropriate compensating security controls.

| **Applicability:** All | **Reference(s):** FISCAM: AC-1, AS-2 | **Related Controls**<br>**Requirement(s):** AC-4, CA-3, MP-4, RA-2 |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-7.1**

**Assessment Objective**

Determine if:

the organization defines the external boundary of the information system;

the organization defines key internal boundaries of the information system;

the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system;

the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

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 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; other relevant documents or records.

## SC-12 – Cryptographic Key Establishment and Management (Low)

**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.

**Guidance**

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

| **Applicability:** All | **Reference(s):** FISCAM: AC-4; IRS-1075: 5.7.1#1 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SC-12.1**

**Assessment Objective**

Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.

**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.

## SC-13 – Use of Cryptography (Low)

**Control**

When cryptographic mechanisms are used, the information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

| | | |
|---|---|---|
| **Applicability:** All | **Reference(s):** FISCAM: AC-4; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2, 5.6.3.4#4.2-3 | **Related Controls Requirement(s):** AC-3, SC-8.Std.1, SC-9(1) |
| **ASSESSMENT PROCEDURE: SC-13.1** | | |
| **Assessment Objective**<br>Determine if when cryptographic mechanisms are used, the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.<br>**Assessment Methods And Objects**<br>**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; other relevant documents or records. | | |
| **SC-13(1) – Enhancement (Low)** | | |
| **Control**<br>When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-13(1).1** | | |
| **Assessment Objective**<br>Determine if when cryptographic mechanisms are used, the organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records. | | |

| SC-14 – Public Access Protections (Low) | | |
|---|---|---|
| **Control**<br>The information system protects the integrity and availability of publicly available information and applications.<br>**Implementation Standard(s)**<br>1. Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.<br>2. If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix D: E-authentication Standard. | | |
| **Guidance**<br>The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.<br>CMS refers to the National Institute of Standards and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix D: E-authentication Standard provides a summary for remote access controls. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2, AC-3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-14.1** | | |
| **Assessment Objective**<br>Determine if:<br>the information system protects the integrity and availability of publicly available information and applications.<br>the organization meets all the requirements specified in the applicable implementation standard(s).<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. | | |

| SC-15 – Collaborative Computing Devices (Low) | | |
|---|---|---|
| **Control**<br>The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system:<br>a. Prohibits remote activation of collaborative computing devices; and<br>b. Provides an explicit indication of use to users physically present at the devices. | | |
| **Guidance**<br>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. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-3 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-15.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative;<br>if authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used;<br>if authorized, the information system prohibits remote activation of collaborative computing devices;<br>if authorized, the information system provides an explicit indication of use to users physically present at the devices. | | |
| **Assessment Methods And Objects**<br>**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. | | |

| SC-20 – Secure Name /Address Resolution Service (Authoritative Source) (Low) | | |
|---|---|---|
| **Control**<br>The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. | | |
| **Guidance**<br>This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. 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. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AC-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-20.1** | | |
| **Assessment Objective**<br>Determine if the information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. | | |
| **SC-20(1) – Enhancement (Low)** | | |
| **Control**<br>The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains. | | |

| | | |
|---|---|---|
| **Guidance**<br>An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SC-20(1).1** | | |
| **Assessment Objective**<br>Determine if:<br>the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces;<br>the information system, when operating as part of a distributed, hierarchical namespace, enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).<br>**Assessment Methods And Objects**<br>**Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. | | |
| **SC-CMS-2 – Website Usage (Low)** | | |
| **Control**<br>CMS web sites are operated within the restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction. | | |
| **Guidance**<br>Monitor the CMS and DHHS security programs to determine is there are any modified directives and instruction. | | |
| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |

| **ASSESSMENT PROCEDURE: SC-CMS-2.1** |
| --- |
| **Assessment Objective**<br>Determine if the organization maintains CMS websites within restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction.<br>**Assessment Methods And Objects**<br>**Examine:** CMS web site baseline and change management documentation for appropriate configurations. |

# 17.0 SYSTEM AND INFORMATION INTEGRITY (SI) – *OPERATIONAL*

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

| **SI-1 – System and Information Integrity Policy and Procedures (Low)** | | |
|---|---|---|
| **Control**<br>The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:<br>a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. | | |
| **Guidance**<br>This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. | | |
| **Applicability:** All | **Reference(s):** FISCAM: AS-1, BP-1, BP-2, BP-3, BP-4, CP-2, SM-1, SM-3; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls Requirement(s):** |
| **ASSESSMENT PROCEDURE: SI-1.1** | | |
| **Assessment Objective**<br>Determine if:<br>the organization develops and formally documents system and information integrity policy; | | |

the organization system and information integrity policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities;

the organization develops and formally documents system and information integrity procedures;

the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls;

the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities.

the organization reviews/updates the system and information integrity policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy and procedures; other relevant documents or records.

**SI-2 – Flaw Remediation (Low)**

**Control**

The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software updates related to flaw remediation for effectiveness and potential side effects on CMS information systems before installation; and
c. Incorporates flaw remediation into the organizational configuration management process.

**Implementation Standard(s)**

1. Correct identified information system flaws on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days.
(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.

**Guidance**

The organization identifies CMS information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) installs security-relevant software updates (e.g., patches, service packs, and hot fixes) within the CMS-designated time period. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in CMS information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts have been accomplished.

| **Applicability:** All | **Reference(s):** FISCAM: AS-3, CM-5; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2 | **Related Controls**<br>**Requirement(s):** CA-2, CA-4, CA-7, CM-3, IR-4, SI-11 |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-2.1**

**Assessment Objective**

Determine if:
the organization identifies, reports, and corrects information system flaws;

the organization tests software updates related to flaw remediation for effectiveness before installation;

the organization tests software updates related to flaw remediation for potential side effects on organizational information systems before installation;

the organization incorporates flaw remediation into the organizational configuration management process.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**SI-2(1) – Enhancement (Low)**

**Control**

The organization centrally manages the flaw remediation process and installs software updates automatically.

**Guidance**

Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-2(1).1**

**Assessment Objective**

Determine if:
the organization centrally manages the flaw remediation process;

the organization installs software updates automatically.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic 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; other relevant documents or records.

**SI-2(2) – Enhancement (Low)**

**Control**

The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-2(2).1**

**Assessment Objective**

Determine if:
the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation;

the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.

**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; other relevant documents or records.

**SI-3 – Malicious Code Protection (Low)**

**Control**

The organization:
a. Employs malicious code protection mechanisms at CMS information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
- Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- Inserted through the exploitation of information system vulnerabilities;
b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with CMS configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
- Perform critical system file scans during system boot, information system scans using the frequency specified in Implementation Standard 1, 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 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 Standard(s)**

1. Desktop malicious code scanning software is configured to perform critical system file scans once a week.

**Guidance**

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong 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 CMS missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

| **Applicability:** All | **Reference(s):** FISCAM: CM-5; IRS-1075: 5.6.2.5#1.3 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-3.1**

**Assessment Objective**

Determine if:

the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code:

- transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- inserted through the exploitation of information system vulnerabilities;

the organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

- transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- inserted through the exploitation of information system vulnerabilities;

the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1;

the organization defines one or more of the following actions to be taken in response to malicious code detection:
- block malicious code;
- quarantine malicious code; and/or
- send alert to administrator;

the organization configures malicious code protection mechanisms to:
- perform periodic scans of the information system in accordance with organization-defined frequency;
- perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;
- take organization-defined action(s) in response to malicious code detection;

the organization addresses the receipt of false positives during malicious code:
- detection and eradication;
- the resulting potential impact on the availability of the information system.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**SI-3(1) – Enhancement (Low)**

**Control**

The organization centrally manages malicious code protection mechanisms.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-3(1).1**

**Assessment Objective**

Determine if the organization centrally manages malicious code protection mechanisms.

**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) – Enhancement (Low)**

**Control**

The information system automatically updates malicious code protection mechanisms (including signature definitions).

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-3(2).1**

**Assessment Objective**

Determine if the information system automatically updates malicious code protection mechanisms, including signature definitions.

**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 (Low) |
|---|
| **Control**<br>The organization:<br>a. Monitors events on the information system in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks;<br>b. Identifies unauthorized use of the information system;<br>c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;<br>d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and<br>e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.<br>**Implementation Standard(s)**<br>1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers. |
| **Guidance**<br>Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). 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, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at 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. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required. |

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, DA-1, SM-5; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4 | **Related Controls Requirement(s):** AC-8, AU-4, CM-6 |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4.1**

**Assessment Objective**

Determine if:
the organization monitors events on the information system in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks;

the organization identifies unauthorized use of the information system;

the organization deploys monitoring devices:
- strategically within the information system to collect organization-determined essential information;
- at ad hoc locations within the system to track specific types of transactions of interest to the organization;

the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

the organization meets all the requirements specified in the applicable 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; other relevant documents or records.

**SI-4(1) – Enhancement (Low)**

**Control**

The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4(1).1**

**Assessment Objective**

Determine if the organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

**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; other relevant documents or records.

**SI-4(5) – Enhancement (Low)**

**Control**

The information system provides near real-time alerts when the following indications of compromise or potential compromise occur:
(a) Presence of malicious code,
(b) Unauthorized export of information,
(c) Signaling to an external information system, or
(d) Potential intrusions.

**Guidance**

Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

| **Applicability:** All | **Reference(s):** | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-4(5).1**

**Assessment Objective**

Determine if:
the organization defines indicators of compromise or potential compromise to the security of the information system;

the information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

**SI-5 – Security Alerts, Advisories, and Directives (Low)**

**Control**

The organization:
a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to appropriate personnel; and
d. Implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.

**Guidance**

Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) 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 affects on CMS operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

| **Applicability:** All | **Reference(s):** FISCAM: AC-5, AS-3, CM-5, DA-1, SM-5 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-5.1**

**Assessment Objective**

Determine if:
the organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;

the organization generates internal security alerts, advisories, and directives;

the organization defines personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives;

the organization disseminates security alerts, advisories, and directives to organization-identified personnel;

the organization implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records.

**SI-8 – Spam Protection (Low)**

**Control**

The organization:
a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with CMS configuration management policy and procedures.

**Guidance**

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers.

| **Applicability:** All | **Reference(s):** FISCAM: CM-5; HIPAA: 164.308(a)(1)(i) | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-8.1**

**Assessment Objective**

Determine if:
the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means;

the organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means;

the organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1.

**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-12 – Information Output Handling and Retention (Low)

**Control**

The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**Implementation Standard(s)**

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 National Archives and Records Administration (NARA) requirements.

**Guidance**

The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention.

| **Applicability:** All | **Reference(s):** FISCAM: BP-2, BP-3; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2 | **Related Controls Requirement(s):** |
|---|---|---|

**ASSESSMENT PROCEDURE: SI-12.1**

**Assessment Objective**

Determine if:

the organization handles both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements;

the organization retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

the organization meets all the requirements specified in the applicable 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.

# CMS Information Security (IS)
# Acceptable Risk Safeguards (ARS)

# Appendix D - CMSR e-Authentication

***(Rev.1, 05-24-11)***

## Table of Contents


**1.0 Introduction** **1**

**2.0 Purpose** **1**

**3.0 E-Authentication Model** **1**

**4.0 Technical Requirements by Assurance Level** **8**

**4.1 Registration and Identity Proofing** **8**

**4.2 Authentication and Mechanism Requirements** **12**

**4.2.1 Token** **13**

**4.3 Summary of Technical Requirements** **19**


## List of Tables


**Table 3-1. e-Authentication Terms, Abbreviations, and Definitions** 3

**Table 4-1. Registration and Identity Proofing** **8**

**Table 4-2. Authentication Mechanism Requirements** **13**

**Table 4-3. Token Types Allowed at Each Assurance Level** **19**

**Table 4-4. Required Protections** **19**

**Table 4-5. Authentication Protocol Types** **20**

**Table 4-6. Additional Required Properties** **20**

**Table A1-1. e-Authentication Assurance Level Definitions** **21**

**Table A1-2. e-Authentication Assurance Level Requirements** **22**

**Table A1-3. Potential Impact Categories and Potential Impact Values** **23**

**Table A1-4. Maximum Assurance Level for each Potential Impact Category** **24**

**Table A1-5. CMS Information Types/Levels & OMB e-Authentication Level Determination** **25**

# Attachments

**Attachment 1—e-Authentication Assurance Levels** **21**

# 1.0 Introduction

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

This appendix contains a broad set of CMS standards based upon National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Electronic Authentication Guideline, V1.0.2, dated April 2006. It provides technical guidance to CMS to allow an individual person to remotely authenticate his/her identity to a CMS information system.

# 2.0 Purpose

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

Federal Information Systems are required to incorporate information security controls to protect the information systems supporting their operations and missions. CMS is required to ensure the adequate protection of its information assets and must meet a minimum level of information security. NIST SP 800-63 supplements OMB guidance, E-Authentication Guidance for Federal Agencies, [OMB 04-04] and defines four (4) levels of assurance for electronic transactions, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. NIST SP 800-63 states specific technical requirements for each of the four (4) levels of assurance.

This document covers remote electronic authentication of human users to CMS information systems over a network. However, it does not address the authentication of a person who is physically present, for example for access to buildings, although some credentials and tokens that are used remotely may also be used for local authentication. Further, this document does not specifically address device-to-device (such as router-to-router) authentication, nor does it establish specific requirements for issuing authentication credentials and tokens to devices and servers when they are used in e-authentication protocols with people.

This document identifies minimum technical requirements for authenticating identity remotely. Business Owners can determine that additional measures are appropriate in certain contexts, based on their risk analysis. In particular, privacy requirements and legal risks may lead Business Owners to determine that additional authentication measures or other process safeguards are appropriate.

# 3.0 E-Authentication Model

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

In accordance with OMB guidance [OMB 04-04], e-authentication is the process of establishing confidence in user identities presented electronically to an information system. Systems can use the authenticated identity to determine whether that individual is authorized to perform an

electronic transaction. In most cases, the authentications and transactions take place across an open network, such as the Internet. However, in some cases access to the network may be limited and access control decisions may take this into account.

E-authentication begins with registration. An applicant applies to a Registration Authority to become a subscriber of a Credential Service Provider (CSP) and, as a subscriber, is issued or registers a secret, called a token, and a credential that binds the token to a name and possibly other attributes that the Registration Authority has verified. The token and credential may be used in subsequent authentication events.

In a common case, the Registration Authority and CSP are separate functions of the same system. However, a Registration Authority might be part of an organization that registers subscribers with an independent CSP, or several different CSPs. Therefore a CSP may have an integral Registration Authority, or it may have relationships with multiple independent Registration Authorities, and a Registration Authority may have relationships with different CSPs as well.

The subscriber's name may either be a verified name or a pseudonym. A verified name is associated with the identity of a real person. Before an applicant can receive credentials or register a token associated with a verified name, he/she must demonstrate that the identity is authentic, and that he/she is the person who is entitled to use that identity. This process is called identity proofing, and is performed by a Registration Authority that registers subscribers with the CSP.

At Level 1, since names are not verified, names are always assumed to be pseudonyms. Level 2 credentials and assertions must specify whether the name is a verified name or a pseudonym. This information assists parties who rely on the name or other authenticated attributes, in making access control or authorization decisions. Only verified names are allowed at Levels 3 and 4. In summary, first an individual applicant applies to a Registration Authority. The Registration Authority identity proofs that applicant. As the result of successful identity proofing, the applicant becomes a subscriber of a CSP associated with the Registration Authority, with a credential and a secret token registered to the subscriber. When the subscriber needs to authenticate to perform a transaction, he/she becomes a claimant to a verifier. The claimant proves to the verifier that s/he controls the token, using an authentication protocol. If the verifier is separate from the relying party (application), the verifier provides an assertion about the claimant to the relying party, which uses the information in the assertion to make an access control or authorization decision. If the transaction is significant, the relying party may log the subscriber identity and credential(s) used in the authentication along with relevant transaction data. Table 3-1 provides e-authentication terms, abbreviations and definitions.

**Table 3-1. e-Authentication Terms, Abbreviations, and Definitions**

| Term or Abbreviation | Definitions |
|---|---|
| Address of Record | The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number, or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available. |
| Attack | An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possess a claimant's token. |
| Attacker | Party who is not the claimant or verifier but who wishes to execute the authentication protocol successfully as a claimant. |
| Approved | FIPS approved or NIST recommended. An algorithm or technique that is either:<br>specified in a FIPS or NIST Recommendation; or<br>adopted in a FIPS or NIST Recommendation.<br>Approved cryptographic algorithms must be implemented in a crypto module validated under FIPS 140-2 (as amended). For more information on validation and a list of validated FIPS 140-2 validated crypto modules see: http://csrc.nist.gov/cryptval/. |
| Assertion | A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol. |
| Asymmetric Keys | Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption, or signature generation and signature verification. |
| Authentication | The process of establishing confidence in user identities. |
| Authentication Protocol | A well-specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected. |
| Authenticity | The quality of data integrity that originates from its purported source. |
| Bit | A binary digit: 0 or 1. |
| Biometric | An image or template of a physiological attribute (e.g., a fingerprint) that may be used to identify an individual. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration. |
| Certification Authority (CA) | A trusted entity that issues and revokes public key certificates. |
| Certificate Revocation List (CRL) | A list of revoked public key certificates created and signed digitally by a Certification Authority. See [RFC 3280] |

| Term or Abbreviation | Definitions |
|---|---|
| Challenge-Response Protocol | An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and independently can compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have authenticated himself successfully. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack. |
| Claimant | A party whose identity is to be verified using an authentication protocol. |
| Credential | An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. |
| Credentials Service Provider (CSP) | A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use. |
| Cryptographic Key | A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number. See also Asymmetric keys, Symmetric key. |
| Cryptographic Strength | A measure of the expected number of operations required to defeat a cryptographic mechanism. For the purposes of this document, this term is defined as meaning that breaking or reversing an operation is at least as difficult computationally as finding the key of an 80-bit block cipher by key exhaustion (it requires at least on the order of 279 operations). |
| Cryptographic Token | A token where the secret is a cryptographic key. |
| Data Integrity | The property that data has not been altered by an unauthorized entity. |
| Digital Signature | An asymmetric key operation where the private key is used digitally to sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. |
| Electronic Credentials | Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document distinguishes between credentials, and tokens (see below) while other documents may interchange these terms. |
| Entropy | A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. |
| FIPS | Federal Information Processing Standard. |
| Guessing Entropy | A measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution. |

| Term or Abbreviation | Definitions |
|---|---|
| Hash Function | A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:<br>1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and<br>2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output. |
| HMAC | Hash-based Message Authentication Code: a symmetric key authentication method using hash functions. |
| Identity | A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique. |
| Identity Proofing | The process by which a CSP and a Registration Authority validate sufficient information to uniquely identify a person. |
| Kerberos | A widely used authentication protocol developed at MIT. In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to-KDC exchange. |
| Man-in-the-Middle Attack (MitM) | An attack on the authentication protocol run in which the attacker is positioned between the claimant and verifier so that he/she can intercept and alter data traveling between them. |
| Message Authentication Code (MAC) | A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. |
| Min-Entropy | A measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system. When a password has n-bits of min-entropy then an attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The attacker is assumed to know the most commonly used password(s). |
| Network | An open communications medium, typically the Internet, which is used to transport messages between the claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party). |
| Nonce | A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement from a random challenge, because a nonce is not necessarily unpredictable. |
| Off-line Attack | An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing. |
| On-line Attack | An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets. |

| Term or Abbreviation | Definitions |
|---|---|
| On-Line Certificate Status Protocol (OCSP) | An on-line protocol used to determine the status of a public key certificate. See [RFC 2560]. |
| Passive Attack | An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e. eavesdropping). |
| Password | A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. |
| Possession and Control of a Token | The ability to activate and use the token in an authentication protocol. |
| Personal Identification Number (PIN) | A password consisting only of decimal digits. |
| Practice Statement | A formal statement of the practices followed by an authentication entity (e.g., Registration Authority, CSP, or verifier); typically, the specific steps taken to register and verify identities, issue credentials, and authenticate claimants. |
| Private Key | The secret part of an asymmetric key pair that typically is used to digitally sign or decrypt data. |
| Proof of Possession (PoP) Protocol | A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password). |
| Protocol Run | An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant. |
| Public Key | The public part of an asymmetric key pair that typically is used to verify signatures or encrypt data. |
| Public Key Certificate | A digital document issued and signed digitally by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See [RFC 3280] |
| Pseudonym | A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing. |
| Registration | The process through which a party applies to become a subscriber of a CSP and a Registration Authority validates the identity of that party on behalf of the CSP. |
| Registration Authority | A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The Registration Authority may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s). |
| Relying Party | An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system. |
| Salt | A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker. |
| Security Assertion Markup Language (SAML) | A specification for encoding security assertions in the XML markup language. |
| Shared Secret | A secret used in authentication that is known to the claimant and the verifier. |
| Subject | The person whose identity is bound in a particular credential. |
| Subscriber | A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol. |

| Term or Abbreviation | Definitions |
|---|---|
| Symmetric Key | A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. |
| Token | Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity. |
| Transport Layer Security (TLS) | An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is similar to the older Secure Socket Layer (SSL) protocol and is effectively SSL version 3.1. |
| Tunneled Password Protocol | A protocol where a password is sent through a protected channel. For example, the TLS protocol is often used with a verifier's public key certificate to:<br>authenticate the verifier to the claimant;<br>establish an encrypted session between the verifier and claimant; and<br>transmit the claimant's password to the verifier.<br>The encrypted TLS session protects the claimant's password from eavesdroppers. |
| Verified Name | A subscriber name that has been verified by identity proofing. |
| Verifier | An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status. |
| Verifier Impersonation Attack | An attack where the attacker impersonates the verifier in an authentication protocol, usually to learn a password. |
| Zero Knowledge Password | Strong password used with special "zero knowledge" protocol. |
| Zero Knowledge Protocol | With Zero-knowledge protocols, someone can convince the verifier that he/she is in possession of the secret without revealing the secret itself, unlike normal username-password queries. |

# 4.0 Technical Requirements by Assurance Level

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

## 4.1 Registration and Identity Proofing

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

In the registration process an applicant undergoes identity proofing by a trusted Registration Authority. If the Registration Authority is able to verify the applicant's identity, the CSP registers or gives the applicant a token and issues a credential as needed to bind that token to the identity or some related attribute. The applicant is now a subscriber of the CSP and may use the token as a claimant in an authentication protocol.

Depending on the assurance level, the registration and identity proofing process is designed to ensure that the Registration Authority / CSP know the true identity of the applicant. Specifically, the requirements include measures to ensure that:

- A person with the applicant's claimed attributes exists, and those attributes are sufficient to identify a single person uniquely;
- The applicant whose token is registered is in fact the person who is entitled to the identity; and
- The applicant cannot later repudiate the registration; therefore, if there is a dispute later about an authentication using the subscriber's token, the subscriber cannot successfully deny he/she registered that token.

In some context, Business Owners may choose to use additional knowledge-based authentication methods to increase their confidence in the registration process. For example, an applicant could be asked to supply non-public information on his or her past dealing with CMS that could help confirm the applicant's identity. Table 4-1 summarizes the registration and identity proofing process.

**Table 4-1. Registration and Identity Proofing**

| Control | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| **1. Registration Requirements** | There are no level-specific requirements at Level 1. | Both in-person and remote registration are permitted.<br>The applicant must supply his | Both in-person and remote registration are permitted.<br>The applicant must supply | Only in-person registration is permitted.<br>The applicant must supply his |

| Control | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | or her full legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS requirements. | his or her full legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS requirements. | or her full legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS requirements. |
| **2. Identity Proofing Requirements** | | | | |
| **2.1. Basis for Issuing Credentials (In-Person)** | There are no level-specific requirements at Level 1. | Possession of a valid current primary Government Picture ID (e.g., driver's license or passport) that contains applicant's picture, and either address of record or nationality | Possession of verified current primary Government Picture ID (e.g., driver's license or passport) that contains applicant's picture and either address of record or nationality | In-person appearance and verification of two (2) independent ID documents or accounts, meeting the requirements of Level 3 (in-person and remote), one of which must be current primary Government Picture ID (e.g., driver's license or passport) that contains applicant's picture, and either address of record or nationality, and a new recording of a biometric of the applicant at the time of application. |
| **2.2. Identity Proofing requirements Registration Authority Actions (In-Person)** | There are no level-specific requirements at Level 1. | Inspect photo-ID, compare picture to applicant, record ID number, address, and date of birth (DoB).<br>If ID appears valid and photo matches applicant then:<br>1) If ID confirms address of record, authorize or issue credentials, and send notice to address of record, or;<br>2) If ID does not confirm address of record, issue credentials in a manner | Inspect Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases.<br>Confirm that: name, DoB, address, and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address, and DoB.<br>If ID is valid and photo | **Primary Photo ID:**<br>Inspect Photo-ID and verify via the issuing government agency, compare picture to applicant, record ID number, address, and DoB.<br>**Secondary Government ID or financial account:**<br>1) Inspect Photo-ID and if apparently valid, compare picture to applicant, record ID number, address, and DoB, or;<br>2) Verify financial account |

| Control | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | that confirms address of record. | matches applicant then:<br>1) If ID confirms address of record, authorize or issue credentials, and send notice to address of record, or;<br>2) If ID does not confirm address of record, issue credentials in a manner that confirms address of record. | number supplied by applicant through record checks or through credit bureaus or similar databases, and confirm that: name, DoB, address, and other personal information in records that are on balance consistent with the application and sufficient to identify a unique individual.<br>**Record Current Biometric:**<br>Record a current biometric (e.g., photograph or fingerprints to ensure that applicant cannot repudiate application.<br>**Confirm Address:**<br>Issue credentials in a manner that confirms address of record. |
| **2.3. Basis for Issuing Credentials (Remote)** | There are no level-specific requirements at Level 1. | Possession of a valid Government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of **either** number. | Possession of a valid Government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of **both** numbers. | **Not Applicable** |
| **2.4. Registration Authority Actions (Remote)** | There are no level-specific requirements at Level 1. | Inspect both ID number and account number supplied by applicant. Verify information provided by applicant including ID number or account number through | Verify information provided by applicant including ID number and account number through record checks either with the applicable agency or institution, or through credit | **Not applicable** |

| Control | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | record checks either with the applicable agency or institution, or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.<br>1) Address confirmation and notification:<br>2) Send notice to an address of record confirmed in the records check or;<br>3) Issue credentials in a manner that confirms the address of record supplied by the applicant; or<br>4) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at a number or e-mail address associated with the applicant in records. | bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual.<br>Address confirmation:<br>1) Issue credentials in a manner that confirms the address of record supplied by the applicant; or<br>2) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice. | |
| **3. Records Retention Requirements** | There are no level-specific requirements at Level 1. | A record of the facts of registration (including revocation) shall be maintained by the CSP or its representative.<br>The minimum record retention period for registration data is **seven (7) years and six (6) months** | A record of the facts of registration (including revocation) shall be maintained by the CSP or its representative.<br>The minimum record retention period for registration data is **seven (7) years and six (6) months** | A record of the facts of registration (including revocation) shall be maintained by the CSP or its representative.<br>The minimum record retention period for registration data **is ten (10) years and six (6) months** |

| Control | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | **beyond the expiration or revocation** (whichever is later) of the credential. | **beyond the expiration or revocation** (whichever is later) of the credential. | **beyond the expiration or revocation** (whichever is later) of the credential. |
| **4. Federal PKI Certificate Policies** | There are no level-specific requirements at Level 1.<br>However, the Public Key Infrastructure (PKI) credentials are not limited to only those certificates by Certification Authorities (CA) cross-certified with the Federal Bridge CA. PKI credentials issued by any CA that has been determined to meet the identity proofing and registration requirements are permitted. | The identity proofing and certificate issuance processes of CAs cross-certified with the Federal Bridge CA (FBCA) under policies mapped to the Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate policies are deemed to meet the identity proofing provisions of this level.<br>However, the PKI credentials are not limited to only those certificates by CAs cross-certified with the FBCA. PKI credentials issued by any CA that has been determined to meet the identity proofing and registration requirements are permitted. | The identity proofing and certificate issuance processes of CAs cross-certified with the FBCA under policies mapped to the Basic, Medium, Medium-HW, or High Certificate polices are deemed to meet the identity proofing provisions of this level.<br>The PKI credentials must be issued by a CA cross-certified with the FBCA under one of the certificate policies identified above or a policy mapped to one of these policies.<br>However, a bi-directional cross-certification is not required; it is sufficient that a valid certificate path exist from the Bridge CA to the issuing CA. The reverse certificate path need not exist. | The identity proofing and certificate issuance processes of CAs cross-certified with the FBCA under policies mapped to the Medium, Medium-HW, or High Certificate policies are deemed to meet the identity proofing provisions of this level.<br>The PKI credentials must be issued by a CA cross-certified with the FBCA under one of the certificate policies identified above or a policy mapped to one of these policies.<br>However, a bi-directional cross-certification is not required; it is sufficient that a valid certificate path exist from the Bridge CA to the issuing CA. The reverse certificate path need not exist. |

## 4.2 Authentication and Mechanism Requirements

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

This section covers the mechanical authentication process of a claimant who already has registered a token. The authentication process shall provide sufficient information to uniquely identify the registration information provided by the subscriber and verified

by the Registration Authority in the issuance of the credential. The technical requirements for authentication mechanisms (tokens, protocols and security protections) are described in this section.

### 4.2.1 Token

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

A token is something that the user possesses and controls (typically a key or password), and used to authenticate the user's identity. Four (4) kinds of tokens for e-authentication are listed in this section. Each type of token incorporates one or more of the authentication factors (something you know, something you have, or something you are). Tokens that provide a higher level of assurance incorporate two or more factors. Tokens are included which focus upon the protection of critical systems. Unauthorized access frequently results in the compromise of system security and information confidentiality.

This recommendation requires multifactor authentication for e-authentication Assurance Levels 3 and 4, and assigns tokens to the four (4) levels corresponding to the OMB guidance. Table 4-2 provides a summary of authentication mechanism requirements.

**NOTE:** When a control for a system is subject to higher standards to meet specific federal, legal, program, accounting, or other requirements, and the system must be developed to meet these higher standards. This document shall not be construed to relieve or waive these other higher standards.

**Table 4-2. Authentication Mechanism Requirements**

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| **1. Token**s | • On-line guessing<br>• Replay | • On-line guessing<br>• Replay<br>• Eavesdropper | • On-line guessing<br>• Replay<br>• Eavesdropper<br>• Verifier impersonation<br>• Man-in-the-Middle | • On-line guessing<br>• Replay<br>• Eavesdropper<br>• Verifier impersonation<br>• Man-in-the-Middle<br>• Session hijacking |
| **1.1. Passwords & PINs** | Employment of a wide range of available authentication technologies is allowed. | The use of any of the token methods of Levels 3 or 4, as well as passwords is | Passwords / PINs may be used as a second level authentication to unlock or | Passwords / PINs may be used as a second level authentication to unlock or |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | The use of any token methods of Levels 2, 3 or 4, as well as passwords is permitted.<br>Common protocols that meet the requirements include APOP [RFC 1939], S/KEY<br>[SKEY], and Kerberos [KERB]. | permitted. | use tokens. | use tokens. |
| **1.2. One-time Password Device Token** | The use of any of the methods of Level 3 is permitted. | The use of any of the methods of Level 3 is permitted. | If used, One-time Password Device Token shall meet the following requirements:<br>• The one-time password output by the device shall have at least 106 possible values.<br>• Passwords must be generated randomly.<br>• The verifier must be authenticated cryptographically to the claimant, for example using a TLS server.<br>• To protect against the use of a stolen token, one of the following measures shall be used:<br>  • The authentication mechanism used to authenticate the claimant to the token shall be validated as meeting the operator authentication requirements for FIPS | **Not Applicable** |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | | | 140-2 Level 2.<br>• The claimant must send the verifier a personal password meeting the requirements for (e-authentication) Level 1 with the one-time password. | |
| **1.3. Software Cryptography Token**<br>(A cryptographic key stored on a general-purpose computer.) | The use of any of the methods of Level 3 is permitted. | The use of any of the methods of Level 3 is permitted. | If used, Software tokens shall meet the following requirements:<br>• The user shall be required to activate the key before using a TLS server.<br>• To protect against the use of a password as well as the key in an authentication protocol with the verifier.<br>• If a personal password meeting the requirements for (e-authentication), and decrypted only for actual use in authentication. Alternatively, if a password protocol is employed with the verifier, the use of the password shall meet the requirements for Level 2 authentication assurance. | **Not Applicable** |
| **1.4. Hardware** | The use of any of the | The use of any of the | If used, Hardware tokens | Hardware tokens shall meet |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| **Cryptography Token** (A cryptographic key stored on a special hardware device) | methods of Level 3 is permitted. | methods of Level 3 is permitted. | shall meet the following requirements:<br>• Tokens must be validated at FIPS 140-2 Level 1 or higher overall.<br>• The user shall be required to activate the key before using it with a password or biometric, or, alternatively shall use a password as well as the key in an authentication protocol with the verifier.<br>• The authentication mechanism used to authenticate the claimant to unlock token shall be validated as meeting the operator authentication requirements for FIPS 140-2 Level 2.<br>• Alternatively, if a password protocol is employed with a verifier, the use of the password shall meet the requirements for Level 1 authentication assurance. | the following requirements:<br>• Token must be validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security.<br>• Requires the entry of a password or a biometric to activate the authentication key.<br>• Must not be able to export authentication keys. |
| **2. Credential / Token Lifetime, Status or Revocation** | The use of any of the methods of Levels 3 or 4 is permitted. | The use of any of the methods of Levels 3 or 4 is permitted. | CSPs shall have a procedure to revoke credentials and tokens within one (1) hour. | CSPs shall have a procedure to revoke credentials immediately after being notified that a credential is no longer valid or a token is compromised. |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| **3. Assertions** | Relying parties may accept assertions that are:<br>• Digitally signed by a trusted entity (e.g., the verifier); or<br>• Obtained directly from a trusted entity (e.g., a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g., TLS) that cryptographically authenticates the verifier and protects the assertion. | Relying parties may accept assertions that are:<br>• Digitally signed by a trusted entity (e.g., the verifier); or<br>• Obtained directly from a trusted entity (e.g., a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g., TLS) that cryptographically authenticates the verifier and protects the assertion.<br>• Assertions generated by a verifier shall expire after twelve (12) hours and should not be accepted thereafter by the relying party. | Relying parties may accept assertions that are:<br>• Digitally signed by a trusted entity (e.g., the verifier); or<br>• Obtained directly from a trusted entity (e.g., a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g., TLS) that cryptographically authenticates the verifier and protects the assertion.<br>• Assertions generated by a verifier shall expire after two (2) hours and should not be accepted thereafter by the relying party. | N/A |
| **4. Protection of Long-Term Shared Secrets** | Files of shared secrets used by verifiers at Level 1 authentication shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such shared secret files shall not contain the plaintext passwords; typically they contain a one-way hash or "inversion" of the password. | Long-term shared authentication secrets, if used, shall never be revealed to any party except the subscriber and CSP, however session (temporary) shared secrets may be provided by the CSP to independent verifiers.<br>Files of shared secrets used by CSPs at Level 2 shall be protected by discretionary access controls that limit | Files of long-term shared secrets used by CSPs or verifiers at Level 3 shall be protected by discretionary access controls that limit access to administrators and only those applications that require access.<br>Such shared secret files shall be encrypted so that:<br>1) The encryption key for the shared secret file is | N/A |

| Controls | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| | In addition, any method allowed for the protection of long-term shared secrets at Levels 2, 3 or 4 may be used at Level 1. | access to administrators and only those applications that require access.<br>Such shared secret files shall not contain the plaintext passwords or secret; two alternative methods may be used to protect the shared secret:<br>1) Passwords may be concatenated to a salt and/or username and then hashed with an Approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file.<br>2) Store shared secrets in encrypted form using approved encryption algorithms and modes. Then decrypt the needed secret, when immediately required for authentication.<br>In addition any method protecting shared secrets, at Level 3 or 4 may be used at Level 2. | encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation.<br>2) Shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module, or any FIPS 140-2 Level 3, or 4 cryptographic modules, and is not exported in plaintext from the module.<br>3) Shared secrets are split by a cryptographic secret sharing method between m separate verifier systems, so that the cooperation of n (where 2 ≦ n ≤ m) systems in a secure protocol is required to perform the authentication and an attacker who learns n-1 of the secret shares, learns nothing about the secret (except, perhaps, its size). | |

## 4.3 Summary of Technical Requirements

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

This section summarizes the technical requirements for each level. Table 4-3 lists the types of tokens that may be used at each assurance level. Table 4-4 identifies the protections that are required at each level. Table 4-5 identifies the types of authentication protocols that are applicable to each assurance level. Table 4-6 identifies additional required protocol and system properties at each level.

**Table 4-3. Token Types Allowed at Each Assurance Level**

| Token Type | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| Hard crypto token | X | X | X | X |
| One-time password device | X | X | X | |
| Soft crypto token | X | X | X | |
| Passwords & PINs | X | X | | |

**Table 4-4. Required Protections**

| Exploits | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| On-line guessing | X | X | X | X |
| Replay | X | X | X | X |
| Eavesdropper | | X | X | X |
| Verifier impersonation | | | X | X |
| Man-in-the-middle | | | X | X |
| Session hijacking | | | | X |

**Table 4-5. Authentication Protocol Types**

| Prototype Type | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| Private Key PoP | X | X | X | X |
| Symmetric key PoP | X | X | X | X |
| Tunneled Password or Zero knowledge password | X | X | | |
| Challenge-reply Password | X | | | |

**Table 4-6. Additional Required Properties**

| Required Property | Levels of Assurance Level 1 | Levels of Assurance Level 2 | Levels of Assurance Level 3 | Levels of Assurance Level 4 |
|---|---|---|---|---|
| Shared secrets not revealed to third parties by verifiers or CSPs | | X | X | X |
| Multi-factor authentication | | | X | X |
| Sensitive data transfer authenticated | | | | X |

# ATTACHMENT 1—E-AUTHENTICATION ASSURANCE LEVELS

***(Rev.1, Issued: 05-24-11, Effective: 08-31-10, Implementation: 06-24-11)***

Office of Management and Budget (OMB) Memorandum 04-04, December 16, 2003, E-Authentication Guidelines for Federal Agencies, defines four (4) levels of authentication (i.e., Levels 1 to 4) required by all Federal agencies for electronic government transactions1. E-Authentication is the process of establishing confidence in user identities electronically presented to an information system. Although not all electronic transactions require authentication, e-Authentication applies to all such transactions for which authentication is required.

OMB defines the required level of authentication assurance (i.e., e-Authentication) in terms of the likely consequences of an authentication error. Each assurance level describes the degree of certainty that the user has presented an identifier (i.e., a credential[2]) that refers to his/her identity. In this context, assurance is defined as: (i) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (ii) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table A1-1 lists the four (4) OMB e-Authentication assurance levels and describes their degree of authentication confidence.

**Table A1-1. e-Authentication Assurance Level Definitions**

| e-Authentication Assurance Level | Definition |
|---|---|
| Level 1 | Little or no confidence in the asserted identity's validity. |
| Level 2 | Some confidence in the asserted identity's validity. |
| Level 3 | High confidence in the asserted identity's validity. |
| Level 4 | Very high confidence in the asserted identity's validity. |

Table A1-2 lists the four (4) e-Authentication assurance levels and describes the degree of authentication, cryptography, and identity proofing required for each level. As the consequences of an authentication error become more serious, the required level of assurance increases.

[1] OMB M-04-04 defines a transaction as: a discrete event between user and systems that supports a business or programmatic purpose.
[2] A credential is defined as: an object that is verified when presented to the verifier in an authentication transaction.

**Table A1-2. e-Authentication Assurance Level Requirements**

| e-Authentication Assurance Level | e-Authentication Requirement |
|---|---|
| Level 1 | • Requires the claimant prove, through a secure authentication protocol that he or she controls a single authentication factor to provide some assurance that the same claimant (who may be anonymous) is accessing the protected transaction.<br>• Little or no confidence exists in the asserted identity.<br>• Cryptography is not required to block offline attacks by an eavesdropper.<br>• No identity proofing is required. |
| Level 2 | • Requires the claimant prove, through a secure authentication protocol that he or she controls a single authentication factor.<br>• Confidence exists that the asserted identity is accurate.<br>• Approved cryptography is required to prevent eavesdroppers.<br>• Identity proofing procedures require presentation of identifying materials or information. |
| Level 3 | • Requires the claimant prove through a cryptographic protocol that he or she controls a minimum of two authentication factors (i.e., multi-factor). Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens, and "one-time password" device tokens. The claimant must unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two-factor authentication.<br>• High confidence exists that the asserted identity is accurate.<br>• Approved cryptography is required for all operations.<br>• Identity proofing procedures require verification of identifying materials and information. |
| Level 4 | • Requires the claimant prove through a cryptographic protocol that he or she controls a minimum of two authentication factors but only "hard" cryptographic tokens are allowed.<br>• Very high confidence exists that the asserted identity is accurate.<br>• Strong, approved cryptographic techniques are used for all operations.<br>• Requires in-person appearance and identity proofing by verification of two independent ID documents or accounts, one of which must be current primary Government picture ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport), and a new recording of a biometric of the applicant. |

The e-Authentication assurance level is determined by assessing the potential risks to CMS and by identifying measures to minimize their impact. The risks from an authentication error are a function of two (2) factors: (i) potential harm or impact, and (ii) the likelihood of such harm or impact, as they apply to six (6) OMB-defined potential impact categories. The potential impact for each of the potential impact categories is assessed using the potential impact values described in FIPS 199 (i.e., High, Moderate, or Low).

Table A1-3 presents the six (6) OMB potential impact categories for authentication errors and their respective potential impact values.

**Table A1-3. Potential Impact Categories and Potential Impact Values**

| Level | Potential impact of "inconvenience, distress or damage to standing or reputation" |
|---|---|
| Low | At worst, limited, short-term inconvenience, distress or embarrassment to any party. |
| Moderate | At worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party. |
| High | Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals). |

| Level | Potential impact of "financial loss" |
|---|---|
| Low | At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability. |
| Moderate | At worst, a serious unrecoverable financial loss to any party, or a serious agency liability. |
| High | Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability. |

| Level | Potential impact of "harm to agency programs or public interests" |
|---|---|
| Low | At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests. |
| Moderate | At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests. |
| High | A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests. |

| Level | Potential impact of "unauthorized release of sensitive information" |
|---|---|
| Low | At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199. |
| Moderate | At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199. |
| High | A release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199. |

| Level | Potential impact of "personal safety" |
|---|---|
| Low | At worst, minor injury not requiring medical treatment. |
| Moderate | At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment. |
| High | A risk of serious injury or death. |

| Level | Potential impact of "civil or criminal violations" |
|---|---|
| Low | At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts. |
| Moderate | At worst, a risk of civil or criminal violations that may be subject to enforcement efforts. |
| High | A risk of civil or criminal violations that are of special importance to enforcement programs. |

The assurance level is determined by comparing the potential impact category to the potential impact value associated with each assurance level, as shown in Table A1-4. The required assurance level is determined by locating the highest level whose impact profile meets or exceeds the potential impact for every impact category.

**Table A1-4. Maximum Assurance Level for each Potential Impact Category**

| | Assurance Level Impact Profiles | | | |
|---|---|---|---|---|
| **Potential Impact Categories** | **1** | **2** | **3** | **4** |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | High |
| Financial loss or agency liability | Low | Mod | Mod | High |
| Harm to agency programs or public interests | N/A | Low | Mod | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | High |
| Personal Safety | N/A | N/A | Low | Mod / High |
| Civil or criminal violations | N/A | Low | Mod | High |

Using the CMS-defined eleven (11) information types and the OMB four (4) e-Authentication assurance levels, a determination was made as to which assurance level impact profile applied to each potential impact category based on the CMS information type. The results of these determinations are included in Table A1-5 and published in CMS System Security and e-Authentication Assurance Levels by Information Types. The basis for determining the overall e-Authentication assurance level for each information type is based on selecting the highest applicable impact level for each information type (refer to the bolded, highlighted levels in Table 12).

If a Business Owner does not agree that the information type processed by their information system requires the same e-Authentication authorization level stated in CMS System Security and e-Authentication Assurance Levels by Information Types, they can use the information and tables provided in this attachment to explain why the assurance level should be different This determination and the reasons for modifying the e-Authentication assurance level must be included in the information system risk assessment and submitted to the CMS CISO for approval prior to using a different e-Authentication level.

Using the e-Authentication assurance level published in CMS System Security and e-Authentication Assurance Levels by Information Types or the assurance level approved by the CMS CSIO, the Business Owner uses Section 4, Technical Requirements by Assurance Level, in Appendix D to apply the necessary requirements to their information system.

## Table A1-5. CMS Information Types/Levels & OMB e-Authentication Level Determination

| Information Type | Explanation and Examples | System Security Level | e-Authentication Level |
|---|---|---|---|
| **Investigation, intelligence-related, and security information (14 CFR PART 191.5(D))** | Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements. | **HIGH**<br>SC = {(confidentiality, **H**), (integrity, **H**), (availability, **M**)} | **Level 4** |

| Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| Inconvenience, distress or damage to standing or reputation | Low | Mod | **Mod** | High |
| Financial loss or agency liability | Low | Mod | **Mod** | High |
| Harm to agency programs or public interests | N/A | Low | **Mod** | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | **High** |
| Personal safety | N/A | **N/A** | Low | Mod / High |
| Civil or criminal violations | N/A | Low | Mod | **High** |

| Information Type | Explanation and Examples | System Security Level | e-Authentication Level |
|---|---|---|---|
| **Mission-critical information** | Information and associated infrastructure directly involved in making payments for Medicare Fee-for-Service (FFS), Medicaid and State Children's Health Insurance Program (SCHIP). | **HIGH**<br>SC = {(confidentiality, **H**), (integrity, **H**), (availability, **H**)} | **Level 4** |

| Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | **High** |
| Financial loss or agency liability | Low | Mod | **Mod** | High |
| Harm to agency programs or public interests | N/A | Low | **Mod** | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | **High** |
| Personal safety | **N/A** | N/A | Low | Mod / High |
| Civil or criminal violations | N/A | Low | **Mod** | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| **Information about persons** | Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). | **MODERATE**<br>SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)} | | **Level 3** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | Low | Mod | **Mod** | High |
| | Financial loss or agency liability | Low | Mod | **Mod** | High |
| | Harm to agency programs or public interests | N/A | Low | **Mod** | High |
| | Unauthorized release of sensitive information | N/A | Low | **Mod** | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | N/A | Low | **Mod** | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| **Financial, budgetary, commercial, proprietary and trade secret information** | Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payments, payroll, automated decision making, procurement, market-sensitive, inventory, other financially-related systems, and site operating and security expenditures. | **MODERATE**<br>SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)} | | **Level 3** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | Low | Mod | **Mod** | High |
| | Financial loss or agency liability | Low | Mod | **Mod** | High |
| | Harm to agency programs or public interests | N/A | Low | **Mod** | High |
| | Unauthorized release of sensitive information | N/A | Low | **Mod** | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | N/A | Low | **Mod** | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| **Internal administration** | Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, advance information concerning procurement actions, management reporting, etc. | **MODERATE**<br>SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)} | | **Level 3** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | Low | **Mod** | Mod | High |
| | Financial loss or agency liability | Low | **Mod** | Mod | High |
| | Harm to agency programs or public interests | N/A | **Low** | Mod | High |
| | Unauthorized release of sensitive information | N/A | Low | **Mod** | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | N/A | **Low** | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| **Other Federal agency information** | Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency. | **MODERATE**<br>SC = {(confidentiality, **M**), (integrity, **M**), (availability, **L**)} | | **Level 3** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | Low | **Mod** | Mod | High |
| | Financial loss or agency liability | Low | **Mod** | Mod | High |
| | Harm to agency programs or public interests | N/A | **Low** | Mod | High |
| | Unauthorized release of sensitive information | N/A | Low | **Mod** | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | N/A | **Low** | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| **New technology or controlled scientific information** | Information related to new technology; scientific information that is prohibited from disclosure or that may require an export license from the Department of State and/or the Department of Commerce. | **MODERATE**<br>SC = {(confidentiality, **M**), (integrity, **M**), (availability, **L**)} | | **Level 3** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | Low | **Mod** | Mod | High |
| | Financial loss or agency liability | Low | **Mod** | Mod | High |
| | Harm to agency programs or public interests | N/A | **Low** | Mod | High |
| | Unauthorized release of sensitive information | N/A | Low | **Mod** | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | N/A | **Low** | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| Operational information | Information that requires protection during operations; usually time-critical information. | **MODERATE**<br>SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)} | | **Level 3** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | Low | **Mod** | Mod | High |
| | Financial loss or agency liability | Low | **Mod** | Mod | High |
| | Harm to agency programs or public interests | N/A | Low | **Mod** | High |
| | Unauthorized release of sensitive information | N/A | Low | **Mod** | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | N/A | **Low** | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| System configuration management information | Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information. | **MODERATE**<br>SC = {(confidentiality, **M**), (integrity, **M**), (availability, **M**)} | | **Level 3** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | Low | Mod | **Mod** | High |
| | Financial loss or agency liability | Low | Mod | **Mod** | High |
| | Harm to agency programs or public interests | N/A | Low | **Mod** | High |
| | Unauthorized release of sensitive information | N/A | Low | **Mod** | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | N/A | Low | **Mod** | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| Other sensitive information | Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare. | **LOW**<br>SC = {(confidentiality, **L**), (integrity, **L**), (availability, **L**)} | | **Level 2** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | Low | **Mod** | Mod | High |
| | Financial loss or agency liability | Low | **Mod** | Mod | High |
| | Harm to agency programs or public interests | N/A | **Low** | Mod | High |
| | Unauthorized release of sensitive information | N/A | **Low** | Mod | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | N/A | **Low** | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | e-Authentication Level | |
|---|---|---|---|---|---|
| Public information | Any information that is declared for public consumption by official authorities and has no identified requirement for integrity or availability. This includes information contained in press releases approved by the Office of Public Affairs or other official sources. | **LOW**<br>SC = {(confidentiality, **L**), (integrity, **L**), (availability, **L**)} | | **Level 1** | |
| | **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| | Inconvenience, distress or damage to standing or reputation | **Low** | Mod | Mod | High |
| | Financial loss or agency liability | **Low** | Mod | Mod | High |
| | Harm to agency programs or public interests | **N/A** | Low | Mod | High |
| | Unauthorized release of sensitive information | **N/A** | Low | Mod | High |
| | Personal safety | **N/A** | N/A | Low | Mod / High |
| | Civil or criminal violations | **N/A** | Low | Mod | High |