Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Appendix A

CMSR High Impact Level Data

FINAL
Version 4.0
March 19, 2009

Document Number: CMS-CIO-STD-SEC01-4.0

(This Page Intentionally Blank)

Access Control (AC) – *Technical*

AC-1 – Access Control Policy and Procedures (High)

Control

Logical access controls and procedures shall be established and implemented effectively to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (i.e., programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

Guidance

The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: AC-1; 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; PISP: 4.1.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents access control policy and procedures;
(ii) the organization disseminates access control policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review access control policy and procedures;
(iv) the organization updates access control policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

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

Interview: Organizational personnel with access control responsibilities.

ASSESSMENT PROCEDURE: AC-1.2

Assessment Objective

Determine if:
(i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;
(iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated access controls.

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

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership;

and assign associated authorizations. Access to the CMS information system shall be granted based on: (a) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (b) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

Implementation Standard(s)

1. Review information system accounts every 90 days and require annual certification.
2. Remove or disable default user accounts. Rename active default accounts.
3. Require the use of unique and separate administrator accounts for administrator and non-administrator activities.
4. Implement centralized control of user access administrator functions.
5. Regulate the access provided to contractors and define security requirements for contractors.
6. Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked prior to or during the termination process.

Guidance

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

Applicability: All	**Reference(s):** ARS: AC-2; 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; PISP: 4.1.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-2.1

Assessment Objective

Determine if:
(i) the organization manages information system accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts;
(ii) the organization defines in the System Security Plan, explicitly or by reference, the frequency of information system account reviews and the frequency is at least annually;
(iii) the organization reviews information system accounts in accordance with organization-defined frequency;
(iv) the organization initiates required actions on information system accounts based on the review.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing account management; System Security Plan; list of active system accounts along with the name of the individual associated with each account; 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

Employ automated mechanisms to support the management of information system accounts.

Applicability: All	**Reference(s):** ARS: AC-2(1); 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

Configure the information system to allow emergency account for a period of time NTE 24 hours and to allow accounts with a fixed duration (i.e., temporary accounts) NTE 365 days.

Applicability: All	**Reference(s):** ARS: AC-2(2); IRS-1075: 5.6.3.2#2.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-2(2).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, a time period for each type of account after which the information system terminates temporary and emergency accounts;

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

Assessment Methods And Objects

Examine: System Security Plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.

AC-2(3) – Enhancement (High)

Control

Configure the information system to disable inactive accounts automatically after 90 days.

Applicability: All	**Reference(s):** ARS: AC-2(3); IRS-1075: 5.6.3.2#2.1	**Related Controls Requirement(s):** IA-4.Std.1

ASSESSMENT PROCEDURE: AC-2(3).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, a time period after which the information system disables inactive accounts;

(ii) the information system automatically disables inactive accounts after organization-defined time period.

Assessment Methods And Objects

Examine: Procedures addressing account management; System Security Plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing account management functions.

AC-2(4) – Enhancement (High)

Control

Employ automated mechanisms to audit user account creation, modification, disabling, and termination. Ensure the automated mechanism notifies appropriate personnel of the user account management actions.

Applicability: All	**Reference(s):** ARS: AC-2(4); IRS-1075: 5.6.3.2#2.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-2(4).1

Assessment Objective

Determine if:
(i) the organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions;

(ii) the organization employs automated mechanisms to notify, 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.

Test: Automated mechanisms implementing account management functions.

AC-3 – Access Enforcement (High)

Control

Access enforcement mechanisms shall be developed, documented and implemented effectively to control access between named users (or processes) and named objects (e.g., files and programs) in a CMS information system. Additional application level access enforcement mechanism shall be implemented, when necessary, to provide increased information security for CMS information. When encryption of stored information is employed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (see section 4.16.13).

In addition, 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.

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, Use of Cryptography, PISP 4.16.13).
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, rule-based policies) and associated 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 controlling 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 a controlled, audited, and manual 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.

Applicability: All	**Reference(s):** ARS: AC-3; 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,	**Related Controls Requirement(s):** MA-CMS-1, MA-CMS-2, SC-13

	5.6.3.3#3; PISP: 4.1.3	

ASSESSMENT PROCEDURE: AC-3.1

Assessment Objective

Determine if:
(i) the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy;

(ii) user privileges on the information system are consistent with the documented user authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of assigned 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

Ensure the information system restricts 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

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Applicability: All	**Reference(s):** ARS: AC-3(1); IRS-1075: 5.6.3.2#2.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-3(1).1

Assessment Objective

Determine if:
(i) the organization explicitly defines privileged functions and security-relevant information for the information system;

(ii) the organization explicitly authorizes personnel access to privileged functions and security-relevant information in accordance with organizational policy;

(iii) the information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel (e.g., security administrators).

Assessment Methods And Objects

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

Test: Automated mechanisms implementing access enforcement policy.

AC-4 – Information Flow Enforcement (High)

Control

Flow control shall be enforced over information between source and destination objects within CMS information systems and between interconnected systems based on the characteristics of the information.

Guidance

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: 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 or provide a packet filtering capability.

Applicability: All	**Reference(s):** ARS: AC-4; FISCAM: AC-1, BP-2, BP-4, DA-1; IRS-1075: 5.6.3.2#2.2; PISP: 4.1.4	**Related Controls Requirement(s):** SC-7

ASSESSMENT PROCEDURE: AC-4.1

Assessment Objective

Determine if the information system enforces assigned 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.

ASSESSMENT PROCEDURE: AC-4.2

Assessment Objective

Determine if interconnection agreements address the types of permissible and impermissible flow of information between information systems and the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system interconnection agreements; list of information flow control authorizations; other relevant documents or records.

AC-5 – Separation of Duties (High)

Control

The principle of separation of duties shall be enforced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission functions and distinct information systems support functions shall be divided among different roles, and support functions shall be performed by different individuals (e.g., personnel responsible for administering access control functions shall not also administer audit functions). Personnel developing and testing system code shall not have access to production libraries. Access control software shall be in place to limit individual authority and information access, such that the collusion of two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties.

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

The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. 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, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Applicability: All	**Reference(s):** ARS: AC-5; 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; PISP: 4.1.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-5.1

Assessment Objective

Determine if:
(i) the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals;

(ii) the information system enforces separation of duties through assigned access authorizations.

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

Each user or process shall be assigned the most restrictive set of privileges needed for the performance of authorized tasks.

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.

Guidance

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 organizational operations, organizational assets, and individuals.

Applicability: All	**Reference(s):** ARS: AC-6; 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; PISP: 4.1.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-6.1

Assessment Objective

Determine if:
(i) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks;

(ii) the information system enforces the most restrictive set of rights/privileges or accesses needed by users.

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-7 – Unsuccessful Log-On Attempts (High)

Control

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce a limit of CMS-defined consecutive invalid access attempts by a user during a specified time period. Systems shall be locked after a specified number of multiple unsuccessful log-on attempts.

Implementation Standard(s)

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

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.

Applicability: All	**Reference(s):** ARS: AC-7; FISCAM: AC-2; IRS-1075: 5.6.3.2#4.1; PISP: 4.1.7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-7.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur;

(ii) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period;

(iii) the organization defines in the System Security Plan, explicitly or by reference, the time period for lock out mode or delay period;

(iv) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts;

(v) the information system enforces the organization-selected lock out mode or delayed login prompt.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing unsuccessful logon attempts; System Security Plan; information system configuration settings and associated documentation.

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

AC-8 – System Use Notification (High)

Control

An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS information system.

Implementation Standard(s)

1. Configure the information system to display a warning banner automatically prior to granting access to potential users. Notify users that:
(a) They are accessing a U.S. Government information system;
(b) CMS maintains ownership and responsibility for its computer systems;

(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
(d) Their usage may be monitored, recorded, and audited;
(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.
2. Develop and implement the warning banner in conjunction with legal counsel.
3. Post clear privacy policies on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.

Guidance

Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Applicability: All	**Reference(s):** ARS: AC-8; FISCAM: AC-1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2; PISP: 4.1.8	**Related Controls Requirement(s):** SI-4

ASSESSMENT PROCEDURE: AC-8.1

Assessment Objective

Determine if:
(i) the information system displays a system use notification message before granting system access informing potential users:
- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording;

(ii) the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries);

(iii) the organization approves the information system use notification message before its use;

(iv) 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; 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 Log-On Notification (High)

Control

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to provide users with information about previous log-ons, both successful and unsuccessful.

Implementation Standard(s)

1. Configure the information system to notify the user, upon successful log-on, of the date and time of the last log-on, and the number of unsuccessful log-on attempts since the last successful log-on.

Guidance

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 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):** ARS: AC-9; FISCAM: AC-1; PISP: 4.1.9	**Related Controls Requirement(s):** AC-

		7.Std.1, CA-4(1), CA-7(1)

ASSESSMENT PROCEDURE: AC-9.1

Assessment Objective

Determine if the information system, upon successful logon, displays the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

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-10 – Concurrent Session Control (High)

Control

Automated mechanisms shall be in place to limit the number of concurrent user sessions, based upon the established business needs of the user, CMS, and the sensitivity level of the CMS information system.

Implementation Standard(s)

1. The number of concurrent User ID network log-on sessions is limited and enforced 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.
2. The requirement and use of more than one (1) application/process session for each user is documented in the SSP.

Guidance

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 periodically review the need for user concurrent sessions.

Applicability: All	**Reference(s):** ARS: AC-10; FISCAM: AC-2, AS-2; PISP: 4.1.10	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-10.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the maximum number of concurrent sessions for information system users;

(ii) the information system limits the number of concurrent sessions for users to the organization-defined number of sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; System Security Plan; other relevant documents or records.

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

AC-11 – Session Lock (High)

Control

Automated session lock mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable locking of the information system session by the user. The information system shall also detect inactivity and block further access until the user re-establishes the connection using proper identification and authentication processes.

Implementation Standard(s)

1. Configure systems to disable local access automatically after fifteen (15) minutes of inactivity. Require a password (see IA-5, Authenticator Management) to restore local access.

Guidance

Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.

Applicability: All	**Reference(s):** ARS: AC-11; FISCAM: AC-1, AS-2; IRS-1075: 5.6.3.2#4.3; PISP: 4.1.11	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-11.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the time period of user inactivity after which the information system initiates a session lock;

(ii) the information system initiates a session lock after the organization-defined time period of inactivity;

(iii) the information system provides the capability for users to directly initiate session lock mechanisms;

(iv) the information system maintains the session lock until the user reestablishes access using appropriate 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; System Security Plan; other relevant documents or records.

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

AC-12 – Session Termination (High)

Control

The information system shall identify and terminate all inactive remote sessions (both user and information system sessions) automatically.

Implementation Standard(s)

1. Configure the information system to automatically terminate all remote sessions (user and information system) after thirty (30) minutes of inactivity.

Guidance

A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Applicability: All	**Reference(s):** ARS: AC-12; FISCAM: AC-1, AS-2; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; PISP: 4.1.12	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-12.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the time period of user inactivity that initiates a remote session termination within the information system;

(ii) the information system automatically terminates a remote session after the organization-defined time period of inactivity.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated

documentation; System Security Plan; other relevant documents or records.

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

AC-12(1) – Enhancement (High)

Control

Automatic session termination applies to local and remote sessions.

Applicability: All	**Reference(s):** ARS: AC-12(1); HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-12(1).1

Assessment Objective

Determine if automatic session termination applies to local and remote sessions.

Assessment Methods And Objects

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

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

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

Control

Personnel shall be supervised and reviewed with respect to the usage of CMS information system access controls. Automated mechanisms shall be in place to facilitate the review of audit records, and any unusual activities shall be investigated in a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of users with significant information system roles and responsibilities shall be reviewed more frequently.

Implementation Standard(s)

1. Review integrity of files and directories for unexpected and/or unauthorized changes at least once per day. Automate the review of file creation, changes and deletions; and monitor permission changes. Generate alert notification for technical staff review and assessment.
2. Enable logging of administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations.
3. Inspect 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

The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**Reference(s):** ARS: AC-13; FISCAM: AC-3, AC-5, AS-4, SD-1, SD-2; HIPAA: 164.308(a)(3)(ii)(A); PISP: 4.1.13	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-13.1

Assessment Objective

Determine if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of

disciplinary actions to users; information system exception reports; other relevant documents or records.

Interview: Organizational personnel with supervisory and access control responsibilities.

AC-13(1) – Enhancement (High)

Control

Employ automated mechanisms to facilitate the review of user activities.

Applicability: All	**Reference(s):** ARS: AC-13(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-13(1).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.

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

Control

Based upon mission / business requirements, public access to CMS information systems without identification and authorization shall be limited to public websites and other publicly available systems. CMS information systems shall be configured 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

The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov).

Applicability: All	**Reference(s):** ARS: AC-14; FISCAM: AC-2, AC-3, AS-2; PISP: 4.1.14	**Related Controls Requirement(s):** IA-2

ASSESSMENT PROCEDURE: AC-14.1

Assessment Objective

Determine if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; System Security Plan; other relevant documents or records.

AC-14(1) – Enhancement (High)

Control

Ensure that public users (users who have not been authenticated) only have access to the extent necessary to accomplish mission objectives while preventing unauthorized access to sensitive information.

Applicability: All	**Reference(s):** ARS: AC-14(1); 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 objectives.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; list of organization-defined actions that can be performed without identification and authentication; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining permitted actions without identification and authentication.

AC-15 – Automated Marking (High)

Control

Automated mechanisms shall be in place to mark CMS information system output using standard naming convention, in order to identify any special dissemination, handling, or distribution instructions.

Guidance

Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used for external marking are distinguished from the labels used on internal data structures described in AC-16.

Applicability: All	**Reference(s):** ARS: AC-15; FISCAM: AC-4; PISP: 4.1.15	**Related Controls Requirement(s):** AC-16

ASSESSMENT PROCEDURE: AC-15.1

Assessment Objective

Determine if:
(i) the organization identifies standard naming conventions for identification of special dissemination, handling, or distribution instructions;
(ii) the information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Assessment Methods And Objects

Examine: Access control policy; procedures for addressing automated marking of information system output; information system output; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining special dissemination, handling, and marking instructions for information system output.

Test: Automated mechanisms implementing automated marking of information system output.

AC-16 – Automated Labeling (High)

Control

CMS information systems shall label information "in storage," "in process," and "in transit" with special dissemination handling or distribution instructions, in a manner consistent with this policy.

Implementation Standard(s)

1. If automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

Guidance

Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.

Applicability: All	**Reference(s):** ARS: AC-16; FISCAM: AC-4; PISP: 4.1.16	**Related Controls Requirement(s):** AC-15

ASSESSMENT PROCEDURE: AC-16.1		
Assessment Objective Determine if the information system appropriately labels information in storage, in process, and in transmission. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test:** Automated mechanisms implementing automated (internal) labeling within the information system.		
AC-17 – Remote Access (High)		
Control Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can access the information system from remote locations shall be limited and justification / approval for such access shall be controlled, documented, and monitored. Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, shall not be used to gain access to a CMS information system that processes CMS sensitive information unless the CIO or his/her designated representative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-up capabilities. **Implementation Standard(s)** 1. Enable secure management protocols through a VPN link(s) if connected to the information system and using remote administration. Utilize an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based). 2. Implement password protection for remote access connections. 3. Require callback capability with re-authentication to verify connections from authorized locations when MDCN 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 every 365 days. 4. If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix D: E-authentication Standard.		
Guidance Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST SP 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 and 800-78. NIST SP 800-77 provides guidance on IPSec-based virtual private networks.		
Applicability: All	**Reference(s):** ARS: AC-17; FISCAM: AC-1, AC-4; IRS-1075: 5.6.3.2#5, 5.7.1#1; PISP: 4.1.17	**Related Controls Requirement(s):** IA-2, SC-9
ASSESSMENT PROCEDURE: AC-17.1		
Assessment Objective Determine if the organization authorizes, monitors, and controls remote access to the information system for all allowed methods of remote access to include both establishment of the remote connection and subsequent user actions across that connection.		

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 (High)

Control

Employ automated mechanisms to facilitate the monitoring and control of remote access methods.

Applicability: All	**Reference(s):** ARS: AC-17(1); 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

Employ cryptography to protect the confidentiality and integrity of remote access sessions.

Applicability: All	**Reference(s):** ARS: AC-17(2); 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 information system employs 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

Control all remote access through a limited number of managed access control points.

Applicability: All	**Reference(s):** ARS: AC-17(3); IRS-1075: 5.6.3.2#5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-17(3).1

Assessment Objective

Determine if:
(i) the organization defines managed access control points for remote access to the information system;
(ii) the information system controls all remote accesses through a limited number of 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

Permit remote access for privileged functions only for compelling operational needs and document the rationale for such access in the security plan for the information system.

Applicability: All	**Reference(s):** ARS: AC-17(4); IRS-1075: 5.6.3.2#5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-17(4).1

Assessment Objective

Determine if:
(i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed;

(ii) the organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the System Security Plan.

Assessment Methods And Objects

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

AC-18 – Wireless Access Restrictions (High)

Control

Installation of wireless access points (WAP) into CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. Authorized WAP devices and wireless access shall be monitored on a regular basis, and wireless communications shall be secured through the use of approved encryption controls.

Implementation Standard(s)

1. CMS policy prohibits the use of wireless access unless explicitly approved by the CMS CIO or his/her designated representative.
2. If wireless access is explicitly approved, wireless devices, 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

NIST SP 800-48 and 800-97 provide guidance on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion detection and prevention.

Applicability: All	**Reference(s):** ARS: AC-18; FISCAM: AC-1, AC-4; PISP: 4.1.18	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-18.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for wireless technologies;

(ii) the organization authorizes, monitors, and controls wireless access to the information system;

(iii) the wireless access restrictions are consistent with NIST Special Publications 800-48 and 800-97.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST Special Publications 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; 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, approved authentication and encryption is used to protect wireless access to the information system.

Applicability: All	**Reference(s):** ARS: AC-18(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-18(1).1

Assessment Objective

Determine if the organization uses authentication and encryption to protect wireless access to the information system.

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

Perform quarterly scans for unauthorized wireless access points and take appropriate action if any access points are discovered.

Guidance

Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.

Applicability: All	**Reference(s):** ARS: AC-18(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-18(2).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of scans for unauthorized wireless access points;

(ii) the organization scans for unauthorized wireless access points in accordance with organization-defined frequency and takes appropriate action if such an access points are discovered.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records.

Test: Scanning procedure for unauthorized wireless access points.

AC-19 – Access Control for Portable and Mobile Devices (High)

Control

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 and networks shall be prohibited unless explicitly authorized, in writing, by the CIO or his/her designated representative. Prior to connecting portable and mobile devices to CMS information systems and networks, such devices shall be configured to comply with CMS IS policies and procedures. The storage and transmission of CMS sensitive information on portable and mobile information devices shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware. The activities and controls shall be commensurate with the system security level of the information.

Implementation Standard(s)

1. If portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative:
Employ an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Guidance

Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, 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). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family.

Applicability: All	**Reference(s):** ARS: AC-19; FISCAM: AC-1; IRS-1075: 4.6#1; PISP: 4.1.19	**Related Controls Requirement(s):** MP-4, MP-5

ASSESSMENT PROCEDURE: AC-19.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices;

(ii) the organization authorizes, monitors, and controls device access to 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-20 – Use of External Information Systems (High)

Control

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 shall not be used to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative.

Strict terms and conditions shall be established for the use of external information systems. The terms and conditions shall address, at a minimum:
4.1.20.1. The types of applications that can be accessed from external information systems;
4.1.20.2. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
4.1.20.3. How other users of the external information system will be prevented from accessing federal information;
4.1.20.4. The use of virtual private networking (VPN) and firewall technologies;
4.1.20.5. The use of and protection against the vulnerabilities of wireless technologies;
4.1.20.6. The maintenance of adequate physical security controls;
4.1.20.7. The use of virus and spyware protection software; and
4.1.20.8. 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 accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.
Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Applicability: All	**Reference(s):** ARS: AC-20; FISCAM: SM-7; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; PISP: 4.1.20	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-20.1

Assessment Objective

Determine if the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

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 FIPS 199 impact level 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

Users are prohibited from using any external information system to access the information system or to process, store, or transmit CMS-controlled information except in situations where the organization:
(a) Can verify the employment of required security controls on the external system as specified in CMS' information security policy and the organization's system 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):** ARS: AC-20(1); IRS-1075: 4.7.2#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-20(1).1

Assessment Objective

Determine if the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:
- verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization's information security policy and System Security Plan when allowing connections to the external information system; or
- approves, for authorized exceptions, 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; System Security Plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records.

AC-CMS-1 – System Boot Access (High)

Control

System boot access shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can alter or perform non-standard boots of systems and/or components of the information system shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Implementation Standard(s)

1. If not explicitly required, boot access to removable media drives is disabled.
2. System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).
3. If not explicitly required, removable media drive functionality is disabled.

Guidance

When a person has unrestrained physical access to any computing system or network device the person has control of the equipment.
If the person does not have the capability to locally access the information system's data though the boot process this can assist in protecting the data from loss or unauthorized access to the data.
Note: Even though the system root access may be protected by privilege access controls a miss configured system can allow the system to reboot and thus allowing a boot / access from unauthorized media. An example of this is a LINUX system, not configured correctly, when CONT+ALT+DEL is issued from the keyboard the equipment will re-boot automatically.

Applicability: All	**Reference(s):** ARS: AC-CMS-1; PISP: 4.1.21	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-CMS-1.1

Assessment Objective

Determine if the organization assesses the need for system boot access and if necessary controls, documents and monitors the continued need for system boot access.

Assessment Methods And Objects

Examine: System boot access documentation to determine that there is or is not a need for boot access.

Interview: Organizational personnel to determine that there is or is not a need for system boot access.

Awareness and Training (AT) – *Operational*

AT-1 – Security Awareness and Training Policy and Procedures (High)

Control

An IS AT program shall be developed, documented, and implemented effectively for all personnel, including contractors and any other users of CMS information and information systems. The IS AT program shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information, information systems, and networks.

Guidance

The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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 information system, when required. NIST SP 800-16 and 800-50 provide guidance on security awareness and training. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: AT-1; FISCAM: AC-6, AS-1, SM-1, SM-3, SM-7; IRS-1075: 5.6.2.7#1.1-2, 6.1#1; PISP: 4.2.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security awareness and training policy and procedures;

(ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review security awareness and training policy and procedures;

(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.

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.

ASSESSMENT PROCEDURE: AT-1.2

Assessment Objective

Determine if:
(i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security awareness and training controls.

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

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS AT program shall be consistent with 5 CFR Part 930 (http://opm.gov/fedregis/2004/69-061404-32835-a.pdf) and the guidance provided in NIST SP 800-50.

Implementation Standard(s)

1. All information system users (including managers and senior executives) receive basic information security awareness training prior to accessing any system's information; when required by system changes; and every 365 days thereafter.
2. Establish a program to promote continuing awareness of information security issues and threats.

Guidance

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	**Reference(s):** ARS: AT-2; FISCAM: AC-6, SM-4; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3; PISP: 4.2.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-2.1

Assessment Objective

Determine if:
(i) the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes;

(ii) the security awareness training is consistent with applicable regulations and NIST Special Publication 800-50;

(iii) the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access;

(iv) the organization defines in the System Security Plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually;

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

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST Special Publication 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; System Security Plan; other relevant documents or records.

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

AT-3 – Security Training (High)

Control

The organization shall identify and document all positions and/or roles with significant information system security responsibilities during the system development life cycle. All personnel with significant information system security responsibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Content of the security awareness training shall be determined based upon the information systems to which personnel have authorized access. The employee shall acknowledge having received the security and awareness training either in writing or electronically as part of the training course completion.

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 every 365 days thereafter.

Guidance

The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel

have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	**Reference(s):** ARS: AT-3; FISCAM: AS-1, SM-4; IRS-1075: 5.6.2.7#1.4; PISP: 4.2.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-3.1

Assessment Objective

Determine if:
(i) the organization identifies personnel with significant information system security responsibilities and roles and documents those roles and responsibilities;

(ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes;

(iii) the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security;

(iv) the security training is consistent with applicable regulations and NIST Special Publication 800-50;

(v) the organization defines in the System Security Plan, explicitly or by reference, the frequency of refresher security training;

(vi) the organization provides refresher security training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST Special Publication 800-50; codes of federal regulations; security training curriculum; security training materials; System Security Plan; other relevant documents or records.

Interview: Organizational personnel with significant information system security responsibilities.

AT-4 – Security Training Records (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that individual IS training activities, including basic security awareness training and specific information system security training, are properly documented and monitored.

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):** ARS: AT-4; FISCAM: AS-1, SM-4; IRS-1075: 6.2#1.3; PISP: 4.2.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-4.1

Assessment Objective

Determine if the organization monitors and documents basic security awareness training and specific information system security training.

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.

AT-5 – Contacts with Security Groups and Associations (High)

Control

Contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations shall be encouraged and supported to enable security personnel to stay up to date with the latest recommended security practices, techniques, and technologies; and to share the latest security-related information including threats, vulnerabilities, and incidents.

Guidance

To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Applicability: All	**Reference(s):** ARS: AT-5; FISCAM: AC-5; HSPD 7: H(25); PISP: 4.2.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-5.1

Assessment Objective

Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security techniques and technologies and to share security-related information.

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.

Audit and Accountability (AU) – *Technical*

AU-1 – Audit and Accountability Policy and Procedures (High)

Control

All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the implementation and management of audit controls, and shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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 information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: AU-1; FISCAM: AS-1, AS-2, SM-1, SM-3; IRS-1075: 5.6.3.3#1; PISP: 4.3.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents audit and accountability policy and procedures;

(ii) the organization disseminates audit and accountability policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review audit and accountability policy and procedures;

(iv) the organization updates audit and accountability policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Audit and accountability policy and procedures; other relevant documents or records.

Interview: Organizational personnel with audit and accountability responsibilities.

ASSESSMENT PROCEDURE: AU-1.2

Assessment Objective

Determine if:
(i) the audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant implementations of all associated audit and accountability controls.

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

Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact

investigations of security incidents. The selection of auditable events shall be based upon a risk assessment as to 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 to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse 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. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**Reference(s):** ARS: AU-2; 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; PISP: 4.3.2	**Related Controls Requirement(s):** AU-4

ASSESSMENT PROCEDURE: AU-2.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, information system auditable events;

(ii) the organization-defined auditable events include those deemed by the organization to be adequate to support after-the-fact investigations of security incidents;

(iii) the information system generates audit records for the organization-defined auditable events;

(iv) the organization specifies which information system components carry out auditing activities;

(v) the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; System Security Plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

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

AU-2(1) – Enhancement (High)

Control

Provide the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical) time correlated audit trail.

Applicability: All	**Reference(s):** ARS: AU-2(1); IRS-1075: 5.6.3.3#2.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-2(1).1

Assessment Objective

Determine if the information system has the capability to compile audit records from the more than one component within the information system into a systemwide (logical or physical), time-correlated audit trail.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing a system-wide auditing capability.

AU-2(2) – Enhancement (High)

Control

Provide the capability to manage the selection of events to be audited by individual components of the information system.

Applicability: All	**Reference(s):** ARS: AU-2(2); IRS-1075: 5.6.3.3#2.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-2(2).1

Assessment Objective

Determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing Information system auditing for the specified components of the information system.

AU-2(3) – Enhancement (High)

Control

Periodically review and update the list of auditable events.

Applicability: All	**Reference(s):** ARS: AU-2(3); IRS-1075: 5.6.3.3#2.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-2(3).1

Assessment Objective

Determine if the organization periodically reviews and updates the list of organization-defined auditable events.

Assessment Methods And Objects

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

Interview: Organizational personnel with auditing and accountability responsibilities.

AU-3 – Content of Audit Records (High)

Control

Automated mechanisms shall be established to provide the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome.

Implementation Standard(s)

1. Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still required.

Guidance

Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST SP 800-92 provides guidance on computer security log management.

Applicability: All	**Reference(s):** ARS: AU-3; FISCAM: AC-5, AS-2, DA-1; IRS-1075: 5.6.3.3#3; PISP: 4.3.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-3.1

Assessment Objective

Determine if:
(i) the information system audit records capture sufficient information to establish what events occurred;

(ii) the information system audit records capture sufficient information to establish the sources of the events;

(iii) the information system audit records capture sufficient information to establish the outcomes of the events.

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

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

Applicability: All	Reference(s): ARS: AU-3(1)	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: AU-3(1).1

Assessment Objective

Determine if the information system provides the capability to include 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; information system design documentation; System 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

Centrally manage the content of audit records generated by individual components throughout the system.

Applicability: All	Reference(s): ARS: AU-3(2)	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: AU-3(2).1

Assessment Objective

Determine if the information system provides the capability to centrally manage the content of audit records generated from multiple components throughout the system.

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

A sufficient amount of information system storage capacity shall be allocated for audit records, and information systems shall be configured to reduce the likelihood of audit records exceeding such storage capacity.

Guidance

The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements.

Applicability: All	Reference(s): ARS: AU-4; FISCAM: AC-5; IRS-1075: 5.6.3.3#4; PISP: 4.3.4	Related Controls Requirement(s): AU-2, AU-5, AU-6, AU-7, SI-4

ASSESSMENT PROCEDURE: AU-4.1

Assessment Objective

Determine if:
(i) the organization allocates sufficient audit record storage capacity;
(ii) 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 (High)

Control

Automated mechanisms shall be established which provide the capability to generate information system alerts for appropriate officials in the event of an audit failure or audit storage capacity being reached and to take appropriate additional actions.

Implementation Standard(s)

1. Alert appropriate officials and take the following actions in response to an audit failure or audit storage capacity issue:
(a) Shutdown the information system,
(b) Stop generating audit records, or
(c) 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):** ARS: AU-5; FISCAM: AC-5, DA-1; PISP: 4.3.5	**Related Controls Requirement(s):** AU-4

ASSESSMENT PROCEDURE: AU-5.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, actions to be taken in the event of an audit processing failure;

(ii) the organization defines in the System Security Plan, explicitly or by reference, personnel to be notified in case of an audit processing failure;

(iii) the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure, to include audit storage capacity being reached or exceeded.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; System Security Plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system response to audit processing failures.

AU-5(1) – Enhancement (High)

Control

The information system provides a warning when allocated audit record storage volume reaches 80% of audit record storage capacity.

Applicability: All	**Reference(s):** ARS: AU-5(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-5(1).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the percentage of maximum audit record storage capacity that, if reached, requires a warning to be provided;

(ii) the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.

Assessment Methods And Objects

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

Test: Automated mechanisms implementing audit storage limit warnings.

AU-5(2) – Enhancement (High)

Control

A second real-time alert is sent when the audit record log is full.

Applicability: All	**Reference(s):** ARS: AU-5(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-5(2).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, audit failure events requiring real-time alerts;

(ii) 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; System 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.

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

Control

Information system audit records shall be reviewed and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and/or suspicious activity. Such activity shall be investigated and reported to appropriate officials, in accordance with current CMS Procedures.

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 staff 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 staff 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 organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Applicability: All	**Reference(s):** ARS: AU-6; 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; PISP: 4.3.6	**Related Controls Requirement(s):** AU-4, IR-4

ASSESSMENT PROCEDURE: AU-6.1

Assessment Objective

Determine if:
(i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity;

(ii) the organization investigates suspicious activity or suspected violations;

(iii) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials;

(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records.

Test: Information system audit monitoring, analysis, and reporting capability.

ASSESSMENT PROCEDURE: AU-6.2

Assessment Objective

Determine if the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, 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 monitoring, analysis, and reporting responsibilities.

AU-6(1) – Enhancement (High)

Control

Employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Applicability: All	**Reference(s):** ARS: AU-6(1); HIPAA: 164.312(b)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-6(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

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

Test: Automated mechanisms integrating audit monitoring, analysis, and reporting into an organizational process for investigation and response to suspicious activities.

AU-6(2) – Enhancement (High)

Control

Employ automated mechanisms to immediately alert security personnel of the following minimal examples of inappropriate or unusual activities with security implications: threats to infrastructure, systems or assets; threats to CMS sensitive data; and threats to finances, personnel, or property.

Applicability: All	Reference(s): ARS: AU-6(2); HIPAA: 164.312(b)	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: AU-6(2).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, inappropriate or unusual activities with security implications;

(ii) the organization employs automated mechanisms to alert security personnel of the occurrence of any organization-defined inappropriate or unusual activities with security implications.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; System Security Plan; information system audit records; other relevant documents or records.

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

Test: Automated mechanisms implementing security alerts.

AU-7 – Audit Reduction and Report Generation (High)

Control

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to enable human review of audit information and the generation of appropriate audit reports.

Guidance

Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Applicability: All	Reference(s): ARS: AU-7; FISCAM: AC-5; PISP: 4.3.7	Related Controls Requirement(s): AU-4

ASSESSMENT PROCEDURE: AU-7.1

Assessment Objective

Determine if the information system provides audit reduction and report generation tools that support after-the-fact investigations of security incidents without altering original audit records.

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 monitoring, analysis, and reporting responsibilities.

Test: Audit reduction and report generation capability.

AU-7(1) – Enhancement (High)

Control

Employ a system capability that automatically processes audit records for events of interest based upon selectable, event criteria.

Applicability: All	Reference(s): ARS: AU-7(1)	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 upon 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; 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

Audit records shall employ time stamps for use in audit record generation. Time stamps of audit records shall be generated using internal system clocks that are synchronized system-wide.

Guidance

Time stamps (including date and time) of audit records are generated using internal system clocks.

Applicability: All	**Reference(s):** ARS: AU-8; FISCAM: AC-5; PISP: 4.3.8	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-8.1

Assessment Objective

Determine if the information system provides time stamps in 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

Information system clock synchronization occurs daily and at system boot.

Applicability: All	**Reference(s):** ARS: AU-8(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-8(1).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of internal clock synchronization for the information system;
(ii) the organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency.

Assessment Methods And Objects

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

Test: Automated mechanisms implementing internal information system clock synchronization.

AU-9 – Protection of Audit Information (High)

Control

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

Guidance

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Applicability: All	Reference(s): ARS: AU-9; FISCAM: AC-5; PISP: 4.3.9	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, and 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-9(1) – Enhancement (High)

Control

Employ automated mechanisms that are restricted to hardware-enforced, "write-once" media for recording audit information (e.g., CD-R, not CD-RW).

Applicability: All	Reference(s): ARS: AU-9(1)	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: AU-9(1).1

Assessment Objective

Determine if the information system produces audit information on hardware-enforced, write-once media.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; other relevant documents or records.

Test: Media storage devices.

AU-10 – Non-Repudiation (High)

Control

Non-repudiation mechanisms shall be implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message.

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 against later false claims by an individual of not having taken a specific action. 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, time stamps).

Applicability: All	Reference(s): ARS: AU-10; FISCAM: AC-2; PISP: 4.3.10	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: AU-10.1

Assessment Objective

Determine if the information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).

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

Audit records shall be retained to provide support for after-the-fact investigations of security incidents, and to meet regulatory and/or CMS information retention requirements. The National Archives and Records Administration maintains criteria for record retention across many disciplines and information security retention standards shall not be construed to relieve or waive these other standards.

Implementation Standard(s)

1. Retain audit records for ninety (90) days, and archive old audit records. Retain audit record archives for one (1) year.
2. (For PII only) Employ mechanisms to facilitate the review of PII disclosure/access records and retain the records for five (5) years or the applicable records control schedule, whichever is longer.
3. (For PII only) To support the audit of 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 PII is stored.
4. (For PII only) 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 the records 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 (CMS sensitive information retention). Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST SP 800-61 provides guidance on computer security incident handling and audit record retention.

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

ASSESSMENT PROCEDURE: AU-11.1

Assessment Objective

Determine if:
(i) the organization defines the retention period for audit records generated by the information system;

(ii) the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Assessment Methods And Objects

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

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

Certification, Accreditation, and Security Assessments (CA) – *Management*

CA-1 – Certification, Accreditation, and Security Assessments Policies and Procedures (High)

Control

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the Business Owner and accredited by the CMS CIO or his/her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the confidentiality, integrity, and availability (CIA) of CMS information and information systems. All C&A and security assessment activities shall be conducted in accordance with current CMS Procedures.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs, MAs, and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and/or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.4.6, Security Accreditation (CA-6).

If the CMS CIO or his/her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his/her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his/her designated representative.

As part of the system certification and accreditation (C&A), an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, IS Risk Assessment (RA), System Security Plan (SSP), independent system tests and evaluations, the Business Owner and System Developer / Maintainer shall certify that the system meets the security requirements to the extent necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CMS CIO or his/her designated representative.

Guidance

The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: CA-1; 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; PISP: 4.4.1	**Related Controls Requirement(s):** CA-6

ASSESSMENT PROCEDURE: CA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security assessment and certification and accreditation policies and procedures;
(ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review policy and procedures;
(iv) the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.

Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.

ASSESSMENT PROCEDURE: CA-1.2

Assessment Objective

Determine if:
(i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security assessment and certification and accreditation controls.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.

Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.

CA-2 – Security Assessments (High)

Control

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application, and comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Routine assessments shall be conducted every 365 days, in accordance with NIST SP 800-53 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. 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 certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.
OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST SP 800-53 A provides guidance on security control assessments to include reuse of existing assessment results.

Applicability: All	**Reference(s):** ARS: CA-2; 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; PISP: 4.4.2	**Related Controls Requirement(s):** CA-4, CA-6, CA-7, CA-7(1), SA-11, SI-2

ASSESSMENT PROCEDURE: CA-2.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of security control assessments and the frequency is at least annually;

(ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency.

Assessment Methods And Objects

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

CA-3 – Information System Connections (High)

Control

Management shall authorize in writing through the use of system connection agreements all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system connections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

Implementation Standard(s)

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

Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST SP 800-47 provides guidance on connecting information systems.

Applicability: All	**Reference(s):** ARS: CA-3; FISCAM: AC-1, SM-1; HSPD 7: F(19); PISP: 4.4.3	**Related Controls Requirement(s):** SA-9, SC-7

ASSESSMENT PROCEDURE: CA-3.1

Assessment Objective

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

(ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements;

(iii) the organization monitors/controls the system interconnections on an ongoing basis.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST Special Publication 800-47; system and communications protection policy; personnel security policy; information system connection agreements; System Security Plan; information system design documentation; information system configuration management and control 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 connection agreements.

CA-4 – Security Certification (High)

Control

Business Owners shall conduct an assessment of the security controls in the information system 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 security certification process shall be integrated into and span across the SDLC. In addition, the Business Owner shall review the certification documentation every 365 days, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his/her designated representative.

Implementation Standard(s)

1. Document the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures.

Guidance

A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation.

Applicability: All	**Reference(s):** ARS: CA-4; FISCAM: AS-1, SM-2, SM-5; HSPD 7: F(19); IRS-1075: 6.3#1.1-2; PISP: 4.4.4	**Related Controls Requirement(s):** CA-2, CA-6, CA-7, SA-11, SI-2

ASSESSMENT PROCEDURE: CA-4.1

Assessment Objective

Determine if:
(i) the organization conducts an assessment of the security controls in the information system 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;

(ii) the organization employs a security certification process in accordance with OMB policy and NIST Special Publications 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; System Security Plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.

Interview: Organizational personnel with security certification responsibilities.

CA-4(1) – Enhancement (High)

Control

Employ an independent certification agent or certification team to conduct an assessment of the information system security controls.

Guidance

An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification 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 certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment of the security controls be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

Applicability: All	**Reference(s):** ARS: CA-4(1); HSPD 7: F(19)	**Related Controls Requirement(s):** AC-9

ASSESSMENT PROCEDURE: CA-4(1).1

Assessment Objective

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

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; security accreditation package (including System Security Plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.

CA-5 – Plan of Action and Milestones (POA&M) (High)

Control

A POA&M shall be developed, implemented, and updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M shall document the planned, implemented, and evaluated corrective actions to repair deficiencies discovered during the security control assessment, and to reduce or eliminate any known vulnerability in the information system.

Personnel shall be designated to assign, track, and update risk mitigation efforts. Designated personnel shall define and authorize corrective action plans, and monitor corrective action progress.

Implementation Standard(s)

1. Develop and submit a plan of action and milestones (POA&M) for any documented information system security finding within thirty (30) days of the final results for every internal / external audit / review or test (e.g., ST&E, penetration test). Update the POA&M monthly until all the findings are resolved.

Guidance

The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems. NIST SP 800-30 provides guidance on risk mitigation.

Applicability: All	**Reference(s):** ARS: CA-5; FISCAM: AS-1, SM-5, SM-6; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4; PISP: 4.4.5	**Related Controls Requirement(s):** CA-7

ASSESSMENT PROCEDURE: CA-5.1

Assessment Objective

Determine if:
(i) the organization develops a plan of action and milestones for the information system;

(ii) the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system;

(iii) the organization defines in the System Security Plan, explicitly or by reference, the frequency of plan of action and milestone updates;

(iv) the organization updates the plan of action and milestones at an organization-defined frequency.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing plan of action and milestones; System 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-6 – Security Accreditation (High)

Control

Explicit authorization to operate the information system shall be received from the CMS CIO or his/her designated representative prior to the system being placed into operations. If the authorization is an interim approval to operate, then the authorization shall be granted based on the designated security category of the information system. An explicit corrective action plan shall be developed, implemented effectively, and monitored by the authorizing official. Re-authorization shall be obtained prior to continued operation:
4.4.6.1. At least every three (3) years;
4.4.6.2. When substantial changes are made to the system;

4.4.6.3. When changes in requirements result in the need to process data of a higher sensitivity;
4.4.6.4. When changes occur to authorizing legislation or federal requirements;
4.4.6.5. After the occurrence of a serious security violation which raises questions about the validity of an earlier certification; and
4.4.6.6. Prior to expiration of a previous accreditation.

Guidance

OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three (3) year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems.

Applicability: All	**Reference(s):** ARS: CA-6; FISCAM: SM-2, SM-5; HSPD 7: F(19); PISP: 4.4.6	**Related Controls Requirement(s):** CA-1, CA-2, CA-4, CA-7

ASSESSMENT PROCEDURE: CA-6.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of authorization updates, not to exceed three years;

(ii) the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization at an organization-defined frequency or when there is a significant change to the information system;

(iii) a senior organizational official signs and approves the security accreditation;

(iv) the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST Special Publication 800-37; security accreditation package (including System Security Plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.

Interview: Organizational personnel with security accreditation responsibilities.

CA-7 – Continuous Monitoring (High)

Control

Security controls in CMS information systems shall be monitored on an on-going basis. Selection criteria for control monitoring shall be established and a subset of the security controls employed within information systems shall be selected for continuous monitoring purposes.

Implementation Standard(s)

1. Continuous monitoring activities include:
(a) Configuration management;
(b) Control of information system components;
(c) Security impact analyses of changes to the system;
(d) On-going assessment of security controls; and
(e) Status reporting.

Guidance

Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation.

Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2).
This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones - the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST SP 800-37 provides guidance on the continuous monitoring process. NIST SP 800-53 A provides guidance on the assessment of security controls.

Applicability: All	**Reference(s):** ARS: CA-7; FISCAM: AS-1, SM-5; HSPD 7: F(19); PISP: 4.4.7	**Related Controls Requirement(s):** CA-2, CA-4, CA-5, CA-6, CM-4, SI-2

ASSESSMENT PROCEDURE: CA-7.1

Assessment Objective

Determine if:
(i) the organization monitors the security controls in the information system on an ongoing basis;

(ii) the organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST Special Publications 800-37 and 800-53A; System Security Plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

Interview: Organizational personnel with continuous monitoring responsibilities.

ASSESSMENT PROCEDURE: CA-7.2

Assessment Objective

Determine if:
(i) the organization conducts security impact analyses on changes to the information system;

(ii) the organization documents and reports changes to or deficiencies in the security controls employed in the information system;

(iii) the organization makes adjustments to the System Security Plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls.

Assessment Methods And Objects

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

Interview: Organizational personnel with continuous monitoring responsibilities.

CA-7(1) – Enhancement (High)

Control

The use of independent certification agents or teams is not required but, if used by the organization to monitor the security controls in the information system on an on-going 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 certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle.

Applicability: All	**Reference(s):** ARS: CA-7(1); HSPD 7: F(19)	**Related Controls Requirement(s):** AC-9, CA-2

ASSESSMENT PROCEDURE: CA-7(1).1

Assessment Objective

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

Assessment Methods And Objects

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

Interview: Organizational personnel with continuous monitoring responsibilities.

Configuration Management (CM) – *Operational*

CM-1 – Configuration Management Policy and Procedures (High)

Control

A CM process that includes the approval, testing, implementation, and documentation of changes shall be developed, documented, and implemented effectively to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with the organization's information technology architecture plans. Formally documented CM roles, responsibilities, procedures, and documentation shall be in place.

Guidance

The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: CM-1; FISCAM: AS-1, CM-1, CP-2, SM-1, SM-3; IRS-1075: 5.6.2.3#1; PISP: 4.5.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents configuration management policy and procedures;

(ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review configuration management policy and procedures;

(iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.

Interview: Organizational personnel with configuration management and control responsibilities.

ASSESSMENT PROCEDURE: CM-1.2

Assessment Objective

Determine if:
(i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated configuration management controls.

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

A baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system shall be developed and documented. Procedures shall

be developed, documented, and implemented effectively to maintain the baseline configuration. The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture.

Implementation Standard(s)

1. Review and, if necessary, update the baseline configuration and any other system-related operations or security documentation at least once every 365 days, and while planning major system changes / upgrades.
2. Maintain an updated list of the information system's operations and security documentation.

Guidance

This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture.

Applicability: All	**Reference(s):** ARS: CM-2; FISCAM: CM-2, CM-3, CM-5, SD-2; HIPAA: 164.310(b); PISP: 4.5.2	**Related Controls Requirement(s):** CM-6, CM-8

ASSESSMENT PROCEDURE: CM-2.1

Assessment Objective

Determine if:
(i) the organization develops and documents a baseline configuration of the information system that is consistent with the Federal Enterprise Architecture, shows relationships among information system components, and provides a well-defined and documented specification to which the information system is built;

(ii) the organization maintains the baseline configuration;

(iii) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.

CM-2(1) – Enhancement (High)

Control

Update the baseline configuration of the information system as an integral part of information system component installations.

Applicability: All	**Reference(s):** ARS: CM-2(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-2(1).1

Assessment Objective

Determine if the organization updates the baseline configuration of the information system as an integral part of information system component installations.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records.

CM-2(2) – Enhancement (High)

Control

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

Applicability: All	**Reference(s):** ARS: CM-2(2)	**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; 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-3 – Configuration Change Control (High)

Control

Change control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to control changes to the information system. Change request forms shall be used to document requests with related approvals. Change requests shall be approved by the Business Owner, or his/her designated representative, and other appropriate organization officials including, but not limited to, the system maintainer and information system support staff.

Test plans shall be developed and approved for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control) and shall include appropriate consideration of security. Test results shall be documented and appropriate responsive actions shall be taken based on the results.

Emergency changes for the CMS information system shall be documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration shall be documented appropriately and approved, and responsible personnel shall be notified for security analysis and follow-up.

Guidance

The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system.

Applicability: All	**Reference(s):** ARS: CM-3; FISCAM: AS-3, BP-2, CM-3, CM-5, CM-6, CP-2; IRS-1075: 5.6.2.3#1; PISP: 4.5.3	**Related Controls Requirement(s):** CM-4, CM-6, SI-2

ASSESSMENT PROCEDURE: CM-3.1

Assessment Objective

Determine if:
(i) the organization authorizes, documents, and controls changes to the information system using an organizationally approved process;

(ii) the organization configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications;

(iii) the organization approves changes to the information system with consideration for the results from the security impact analysis of the change;

(iv) the organization audits activities associated with configuration changes to the information system.

Assessment Methods And Objects

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

CM-3(1) – Enhancement (High)

Control

Employ automated mechanisms to:
(a) Document proposed changes to the information system,
(b) Notify appropriate approval authorities,
(c) Identify approvals that have not been received in a timely manner,
(d) Inhibit change until necessary approvals are received, and
(e) Document completed changes to the information system.

Applicability: All	**Reference(s):** ARS: CM-3(1); IRS-1075: 5.6.2.3#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-3(1).1

Assessment Objective

Determine if:
(i) the organization employs automated mechanisms to document proposed changes to the information system;
(ii) the organization employs automated mechanisms to notify appropriate approval authorities;
(iii) the organization employs automated mechanisms to highlight approvals that have not been received in a timely manner;
(iv) the organization employs automated mechanisms to inhibit change until necessary approvals are received;
(v) the organization employs automated mechanisms to document completed changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; 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-4 – Monitoring Configuration Changes (High)

Control

Mechanisms to monitor change activity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to monitor information system changes and actions by privileged users. Security impact analyses shall be conducted after system changes are made to determine the IS-related effects of the changes. Activities associated with configuration changes to the information system shall be audited.

Implementation Standard(s)

1. When changes to the system occur, record the installation of information system components in the appropriate system documentation resource(s).

Guidance

Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system.

Applicability: All	**Reference(s):** ARS: CM-4; FISCAM: AS-3, CM-3, CM-4, SM-5; PISP: 4.5.4	**Related Controls Requirement(s):** CA-7, CM-3

ASSESSMENT PROCEDURE: CM-4.1

Assessment Objective

Determine if the organization monitors changes to the information system by verifying that the organization:
- prior to change implementation and as part of the change approval process, conducts security impact analyses to assess the effects of the system changes;
- after the system is changed (including upgrades and modifications), checks the security features to confirm that the features are still functioning properly;
- audits activities associated with configuration changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

CM-5 – Access Restrictions for Change (High)

Control

Access control change mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to approve individual access privileges and to enforce physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.

Guidance

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

Applicability: All	**Reference(s):** ARS: CM-5; FISCAM: AC-4, AS-3, CM-3, CM-4; IRS-1075: 5.6.2.3#1; PISP: 4.5.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-5.1

Assessment Objective

Determine if:
(i) the organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system, including upgrades, and modifications;

(ii) the organization generates, retains, and reviews records reflecting all such changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; 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 responsible for generating, retaining, and reviewing records reflecting changes to the information system.

Test: Change control process and associated restrictions for changes to the information system.

CM-5(1) – Enhancement (High)

Control

Employ automated mechanisms to enforce access restrictions and to support auditing of the enforcement actions.

Applicability: All	**Reference(s):** ARS: CM-5(1); IRS-1075: 5.6.2.3#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-5(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

Assessment Methods And Objects

Examine: Configuration management policy; 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.

Test: Automated mechanisms implementing access restrictions for changes to the information system.

CM-6 – Configuration Settings (High)

Control

Procedures shall be developed, documented, and implemented effectively to configure and benchmark information technology products in accordance with good security practice settings. Mandatory configuration settings for information technology products employed within the information system shall be established. The security settings of information technology products shall be configured to the most restrictive mode consistent with information system operational requirements, documented, and enforced in all components of the information system.

Implementation Standard(s)

1. Configure the information system to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

Guidance

Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems.

Applicability: All	**Reference(s):** ARS: CM-6; FISCAM: AC-3, AS-3, CM-2, CM-3; IRS-1075: 5.6.2.3#1; PISP: 4.5.6	**Related Controls Requirement(s):** CM-2, CM-3, CM-8, SI-4

ASSESSMENT PROCEDURE: CM-6.1

Assessment Objective

Determine if:
(i) the organization establishes mandatory configuration settings for information technology products employed within the information system;
(ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;
(iii) the organization documents the configuration settings;
(iv) the organization enforces the configuration settings in all components of the information system;
(v) the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST Special Publication 800-70; other relevant documents or records.

Interview: Organizational personnel with security configuration responsibilities.

CM-6(1) – Enhancement (High)

Control

Employ automated mechanisms to centrally manage, apply, and verify configuration settings.

Applicability: All	Reference(s): ARS: CM-6(1); IRS-1075: 5.6.2.3#1	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: CM-6(1).1

Assessment Objective

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

Assessment Methods And Objects

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

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

CM-7 – Least Functionality (High)

Control

Information systems shall be configured to provide only essential capabilities. The functions and services provided by CMS information systems shall be reviewed carefully to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol [VoIP], Instant Messaging [IM], File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP], file sharing). The use of those functions, ports, protocols, and/or services shall be prohibited and/or restricted.

Implementation Standard(s)

1. Configure the information system specifically to only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system / 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 organizational 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, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Applicability: All	Reference(s): ARS: CM-7; FISCAM: AC-3, CM-3; IRS-1075: 5.6.2.3#1; PISP: 4.5.7	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: CM-7.1

Assessment Objective

Determine if:

(i) the organization defines in the System Security Plan, explicitly or by reference, prohibited or restricted functions, ports, protocols, and services for the information system;

(ii) the organization configures the information system to provide only essential capabilities;

(iii) the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined functions, ports, protocols, and/or services.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; System Security Plan; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for disabling or restriction of functions, ports, protocols, and services.

CM-7(1) – Enhancement (High)

Control

Review the information system every 365 days or on an incremental basis where all parts are addressed within a year, to identify and eliminate unnecessary functions, ports,

protocols, and/or services.

Applicability: All	**Reference(s):** ARS: CM-7(1); IRS-1075: 5.6.2.3#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-7(1).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of the information system reviews to identify and eliminate unnecessary functions, ports, protocols, and services;

(ii) the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; System Security Plan; information system configuration settings and associated documentation; 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 (High)

Control

Procedures shall be developed, documented, and implemented effectively to document and maintain a current inventory of the information system's constituent components and relevant ownership information. The inventory of information system components shall include manufacturer, model / type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership.

Guidance

The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system.

Applicability: All	**Reference(s):** ARS: CM-8; FISCAM: CM-2, SM-1; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); PISP: 4.5.8	**Related Controls Requirement(s):** CM-2, CM-6

ASSESSMENT PROCEDURE: CM-8.1

Assessment Objective

Determine if:
(i) the organization develops and documents an inventory of the components of the information system:
- that is at the level of granularity deemed appropriate by the organization for the components included in the inventory that are subject to tracking and reporting;
- that includes any information determined to be necessary by the organization to achieve effective property accountability;
- that is consistent with the accreditation boundary of the system;

(ii) the organization maintains the inventory of the components of the information system to reflect the current state of the system.

Assessment Methods And Objects

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

CM-8(1) – Enhancement (High)

Control

Update the information system component inventory as an integral part of component installations.

Applicability: All	**Reference(s):** ARS: CM-8(1); 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.

Assessment Methods And Objects

Examine: Configuration management policy; 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

Employ automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Applicability: All	**Reference(s):** ARS: CM-8(2); HIPAA: 164.310(d)(1), 164.310(d)(2)(iii)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-8(2).1

Assessment Objective

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

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records.

Test: Automated mechanisms implementing information system component inventory management.

Contingency Planning (CP) – *Operational*

CP-1 – Contingency Planning Policy and Procedures (High)

Control

All major CMS information systems shall be covered by a CP that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

Guidance

The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-34 provides guidance on contingency planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: CP-1; 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; PISP: 4.6.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents contingency planning policy and procedures;
(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review contingency planning policy and procedures;
(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with contingency planning responsibilities.

ASSESSMENT PROCEDURE: CP-1.2

Assessment Objective

Determine if:
(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;
(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated contingency planning controls.

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

All major CMS information systems shall be covered by a CP, relative to the system security level, providing continuity of support in the event of a disruption of service. A CP for

the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A CP for the information system shall be consistent with NIST SP 800-34. Designated officials within the organization shall review and approve the CP and distribute copies of the plan to key contingency personnel.

Guidance

Contingency Plans consist of all components listed in the CMS Business Partners system Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.

Applicability: All	**Reference(s):** ARS: CP-2; 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; PISP: 4.6.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-2.1

Assessment Objective

Determine if:
(i) the organization develops and documents a contingency plan for the information system;

(ii) the contingency plan is consistent with NIST Special Publication 800-34;

(iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure;

(iv) the contingency plan is reviewed and approved by designated organizational officials;

(v) the organization disseminates the contingency plan to key contingency personnel.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; NIST Special Publication 800-34; contingency plan; other relevant documents or records.

CP-2(1) – Enhancement (High)

Control

Coordinate development of the Contingency Plan (CP) with parties responsible for related plans, such as the Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan (COOP), Business Recovery Plan, and Incident Response Plan.

Guidance

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

Applicability: All	**Reference(s):** ARS: CP-2(1); 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 with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

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

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

Applicability: All	**Reference(s):** ARS: CP-2(2); HSPD 7: G(22)(i)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-2(2).1

Assessment Objective

Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-3 – Contingency Training (High)

Control

Operational and support personnel (including managers and users of the information system) shall receive training in contingency operations and understand their contingency roles and responsibilities with respect to the information system. Refresher training shall be provided to all contingency personnel.

Implementation Standard(s)

1. Provide training every 365 days in contingency roles and responsibilities.

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):** ARS: CP-3; FISCAM: CP-2; HSPD 7: G(22)(i); PISP: 4.6.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-3.1

Assessment Objective

Determine if:
(i) the organization provides contingency training to personnel with contingency roles and responsibilities;

(ii) the organization defines in the System Security Plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is at least annually;

(iii) the organization provides initial training and 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; System Security Plan; contingency training records; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

ASSESSMENT PROCEDURE: CP-3.2

Assessment Objective

Determine if contingency training material addresses the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.

CP-3(1) – Enhancement (High)

Control

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Applicability: All	**Reference(s):** ARS: CP-3(1); HSPD 7: G(22)(i)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-3(1).1

Assessment Objective

Determine if:
(i) the organization incorporates simulated events into contingency training;

(ii) the incorporation of simulated events into contingency training facilitates effective response by personnel in crisis situations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-3(2) – Enhancement (High)

Control

Employ automated mechanisms to provide thorough and realistic training environments.

Applicability: All	**Reference(s):** ARS: CP-3(2); HSPD 7: G(22)(i)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-3(2).1

Assessment Objective

Determine if the organization employs automated mechanisms that provide a more thorough and realistic contingency training environment.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; automated mechanisms supporting contingency training; contingency training curriculum; contingency training material; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-4 – Contingency Plan Testing and Exercises (High)

Control

CPs shall be tested and/or exercised at least every 365 days using defined tests and exercises, such as the tabletop test in accordance with current CMS Procedures, to determine the plans' effectiveness and readiness to execute the plan. Test / exercise results shall be documented and reviewed by appropriate organization officials. Reasonable and appropriate corrective actions shall be initiated to close or reduce the impact of CP failures and deficiencies.

Implementation Standard(s)

1. The CP must be current and executable, tested using a combination of tabletop exercises and operational tests every 365 days, and updated as needed.

Guidance

There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop

exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Applicability: All	**Reference(s):** ARS: CP-4; 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; PISP: 4.6.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-4.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted;
(ii) the organization defines in the System Security Plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is at least annually;
(iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;
(iv) 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; System 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.

ASSESSMENT PROCEDURE: CP-4.2

Assessment Objective

Determine if:
(i) the contingency plan tests/exercises confirm the plan's effectiveness;
(ii) the contingency plan tests/exercises confirm the organization's readiness to execute the plan;
(iii) the contingency plan tests/exercises confirm the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

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(1) – Enhancement (High)

Control

Coordinate testing and exercising of CP with parties responsible for related plans, such as:
(a) Business Continuity Plan,
(b) Disaster Recovery Plan,
(c) Continuity of Operations Plan,
(d) Business Recovery Plan, and
(e) Incident Response Plan.

Guidance

Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

Applicability: All	**Reference(s):** ARS: CP-4(1); 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 (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

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.

CP-4(2) – Enhancement (High)

Control

Test / exercise the CP at the alternate processing site to evaluate the site's capabilities to support contingency operations.

Applicability: All	**Reference(s):** ARS: CP-4(2); 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 at the alternate processing site to familiarize contingency personnel with the facility and its 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(3) – Enhancement (High)

Control

Employ automated mechanisms to more thoroughly and effectively test / exercise the CP by providing more complete coverage of contingency issues, selecting more realistic test / exercise scenarios and environments, and more effectively stressing the information system and supported missions.

Applicability: All	**Reference(s):** ARS: CP-4(3); HSPD 7: G(22)(i)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-4(3).1

Assessment Objective

Determine if the organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; automated mechanisms supporting contingency plan testing/exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.

CP-5 – Contingency Plan Update (High)

Control

CPs shall be reviewed at least every 365 days and, if necessary, revised to address system / organizational changes and/or any problems encountered during plan implementation, execution, or testing.

Guidance

Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Applicability: All	**Reference(s):** ARS: CP-5; FISCAM: AS-5, CP-3, CP-4; HSPD 7: G(22)(i); PISP: 4.6.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-5.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of contingency plan reviews and updates and the frequency is at least annually;

(ii) the organization reviews the contingency plan in accordance with organization-defined frequency;

(iii) the organization updates the contingency plan as necessary to addresses the system/organizational changes identified by the organization or any problems encountered by the organization during plan implementation, execution, and testing.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; System Security Plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-5.2

Assessment Objective

Determine if the organization communicates necessary changes to the contingency plan to other organizational elements with related plans.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records.

Interview: Organizational personnel with contingency plan update responsibilities; organizational personnel with mission-related and operational responsibilities.

CP-6 – Alternate Storage Site (High)

Control

Agreements with an alternate storage site shall be established and implemented effectively to permit the storage of CMS information system backup information. Copies of the current CP shall be stored in a secure location at an alternate site accessible by management and other key personnel. Procedures shall be developed, documented, and implemented effectively to respond to contingencies by ensuring separation of routine information system operations and the alternate storage site.

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 the organization's recovery time objectives and recovery point objectives.

Applicability: All	**Reference(s):** ARS: CP-6; FISCAM: AS-5, CP-2, CP-3; IRS-1075: 5.6.2.2#1.4; PISP: 4.6.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-6.1

Assessment Objective

Determine if:
(i) the organization identifies an alternate storage site;

(ii) the organization initiates necessary alternate storage site agreements to permit storage 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

Ensure that the alternate storage site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.

Applicability: All	**Reference(s):** ARS: CP-6(1); IRS-1075: 5.6.2.2#1.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-6(1).1

Assessment Objective

Determine if:
(i) the contingency plan identifies the primary storage site hazards;
(ii) the alternate storage site is sufficiently 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

Ensure that the alternate storage site is configured to facilitate timely and effective recovery operations.

Applicability: All	**Reference(s):** ARS: CP-6(2); 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 enable timely and effective recovery operations.

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

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and document explicit mitigation actions.

Applicability: All	**Reference(s):** ARS: CP-6(3); IRS-1075: 5.6.2.2#1.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-6(3).1

Assessment Objective

Determine if:
(i) the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster;
(ii) the organization defines explicit mitigation actions for potential accessibility problems.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

CP-7 – Alternate Processing Site (High)

Control

Agreements with an alternate processing site shall be established and implemented to permit the resumption of CMS information system operations for mission critical business functions when the primary processing capabilities are unavailable, and the CP calls for application recovery in place of other accepted processes. Procedures shall be developed, documented, and implemented effectively to establish contingency activities and responsibilities.

Implementation Standard(s)

1. Ensure all equipment and supplies required for resuming information system operations for critical functions are available within one week at the alternate processing site, or contracts are in place to support delivery to the site.

Guidance

Equipment and supplies required to resume operations within the organization-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 organization-established recovery time objectives.

Applicability: All	**Reference(s):** ARS: CP-7; FISCAM: CP-2, CP-3; IRS-1075: 5.6.2.2#1.5; PISP: 4.6.7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-7.1

Assessment Objective

Determine if:
(i) the organization identifies an alternate processing site;

(ii) the organization defines in the System Security Plan, explicitly or by reference, the time period within which processing must be resumed at the alternate processing site;

(iii) the organization initiates necessary alternate processing site agreements to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; System Security Plan; other relevant documents or records.

CP-7(1) – Enhancement (High)

Control

Ensure the alternate processing site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.

Applicability: All	**Reference(s):** ARS: CP-7(1); IRS-1075: 5.6.2.2#1.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-7(1).1

Assessment Objective

Determine if:
(i) the contingency plan identifies the primary processing site hazards;

(ii) the alternate processing site is sufficiently 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

Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Applicability: All	Reference(s): ARS: CP-7(2); IRS-1075: 5.6.2.2#1.5	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: CP-7(2).1

Assessment Objective

Determine if:
(i) the contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster;
(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.

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

Ensure alternate processing site agreements contain appropriate priority-of-service provisions.

Applicability: All	Reference(s): ARS: CP-7(3); 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(4) – Enhancement (High)

Control

Ensure the alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.

Applicability: All	Reference(s): ARS: CP-7(4); IRS-1075: 5.6.2.2#1.5	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: CP-7(4).1

Assessment Objective

Determine if the alternate processing site is configured to support the minimum required information system operational capability and is ready to use as the operational site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records.

Test: Information system at the alternate processing site.

CP-8 – Telecommunications Services (High)

Control

Necessary agreements shall be established and implemented for alternate communications services capable of restoring adequate communications to accomplish mission critical functions when the primary operations and communications capabilities are unavailable.

Implementation Standard(s)

1. Resume system operations for critical functions within one week when the primary telecommunications capabilities are unavailable.

Guidance

In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).

Applicability: All	**Reference(s):** ARS: CP-8; FISCAM: CP-2, CP-3; IRS-1075: 5.6.2.2#1.5; PISP: 4.6.8	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-8.1

Assessment Objective

Determine if:
(i) the organization identifies primary and alternate telecommunications services to support the information system;

(ii) the organization defines in the System Security Plan, explicitly or by reference, the time period within which resumption of information system operations must take place;

(iii) the organization initiates necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for critical mission/business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; System Security Plan; primary and alternate telecommunications service agreements; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-8.2

Assessment Objective

Determine if the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness when 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; other relevant documents or records.

CP-8(1) – Enhancement (High)

Control

Ensure agreements with primary and alternate telecommunication service providers include priority-of-service provisions.

Applicability: All	**Reference(s):** ARS: CP-8(1); 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.

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.

CP-8(2) – Enhancement (High)

Control

Ensure alternate telecommunication providers do not share a single point of failure with primary telecommunications services.

Applicability: All	**Reference(s):** ARS: CP-8(2); 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 that do not share 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

Ensure alternate telecommunications service providers are sufficiently separated from the primary telecommunications services, to prevent susceptibility to the same hazards.

Applicability: All	**Reference(s):** ARS: CP-8(3); IRS-1075: 5.6.2.2#1.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-8(3).1

Assessment Objective

Determine if the organization obtains alternate telecommunications service that is sufficiently separated from the primary provider's telecommunications service 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

Ensure that primary and alternate telecommunication service providers have adequate CPs.

Applicability: All	**Reference(s):** ARS: CP-8(4); IRS-1075: 5.6.2.2#1.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-8(4).1

Assessment Objective

Determine if the organization requires primary and alternate telecommunications service providers to have contingency plans deemed adequate by the organization.

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, plan implementation, and testing responsibilities; telecommunications service providers.

CP-9 – Information System Backup (High)

Control

Backup mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable the backing-up of user-level and system-level information (including system state information) contained in the CMS information system. The frequency of information system backups and the transfer rate of backup information to an alternate storage site (if so designated) shall be consistent with the CMS recovery time objectives and recovery point objectives.

Mechanisms shall provide for sufficient backup storage capability. Checkpoint capabilities shall be part of any backup operation that updates files and consumes large amounts of information system time. Backup copies of CMS data shall be created on a regular basis, and appropriate safeguards shall be implemented to protect the technical and physical security of backup media at the storage location. Where appropriate, backup copies of all other forms of data, including paper records, shall be created based upon an assessment of the level of data criticality and the corresponding risk of data loss.

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 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

The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time. The protection of system backup information while in transit is beyond the scope of this control.

Applicability: All	**Reference(s):** ARS: CP-9; FISCAM: AS-5, CP-2; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6; PISP: 4.6.9	**Related Controls Requirement(s):** MA-CMS-1, MA-CMS-2, MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9.1

Assessment Objective

Determine if:
(i) the organization defines the frequency of information systems backups;

(ii) the organization backs up user-level and system-level information (including system state information) in accordance with the organization-defined frequency;

(iii) the organization backs up information to alternate storage sites (if so designated) at a frequency and transfer rate consistent with the organization's recovery time objectives and recovery point objectives.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; System Security Plan; backup storage location(s); other relevant documents or records.

ASSESSMENT PROCEDURE: CP-9.2

Assessment Objective

Determine if the organization protects backup information at the designated storage locations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; System Security Plan; backup storage location(s); other relevant documents or records.

CP-9(1) – Enhancement (High)

Control

Test backup information to verify media reliability and information integrity, following each backup.

Applicability: All	**Reference(s):** ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-9(1).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of information system backup testing;

(ii) the organization conducts information system backup testing in accordance with organization-defined frequency;

(iii) testing results verify backup media reliability and information integrity.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; System Security Plan; information system backup test results; backup storage location(s); other relevant documents or records.

CP-9(2) – Enhancement (High)

Control

Use select backup information to restore information systems as part of the Contingency Plan testing.

Applicability: All	**Reference(s):** ARS: CP-9(2); 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 selected backup information in the restoration of 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 test results; other relevant documents or records.

CP-9(3) – Enhancement (High)

Control

Ensure that backup copies of the operating system and other critical information system software are stored at a separate facility or in a fire-rated container that is not collocated with operational software.

Applicability: All	**Reference(s):** ARS: CP-9(3); 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 in a separate facility or in a fire-rated container that is not collocated with the operational software.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; backup storage location(s); other relevant documents or records.

CP-9(4) – Enhancement (High)

Control

Protect backup information from unauthorized modification.

Guidance

The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control.

Applicability: All	Reference(s): ARS: CP-9(4); IRS-1075: 5.6.2.2#1.6	Related Controls Requirement(s): MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9(4).1

Assessment Objective

Determine if the organization employs appropriate mechanisms to protect the integrity of information system backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; backup storage location(s); information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with information system backup responsibilities.

CP-10 – Information System Recovery and Reconstitution (High)

Control

Information system recovery and reconstitution mechanisms with supporting procedures shall be developed, documented, and implemented effectively to allow the CMS information system to be recovered and reconstituted to a known secure state after a disruption or failure. Recovery of CMS information systems after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

Implementation Standard(s)

1. Secure information system recovery and reconstitution includes, but not limited to:
(a) Reset all system parameters (either default or organization-established),
(b) Reinstall patches,
(c) Reestablish configuration settings,
(d) Reinstall application and system software, and
(e) Fully test the system.

Guidance

Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Applicability: All	Reference(s): ARS: CP-10; FISCAM: CP-2, CP-3, CP-4; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); PISP: 4.6.10	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: CP-10.1

Assessment Objective

Determine if the organization provides and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.

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 implementing information system recovery and reconstitution operations.

CP-10(1) – Enhancement (High)

Control

Perform full recovery and reconstitution of the information system as part of CP testing.

Applicability: All	**Reference(s):** ARS: CP-10(1); HSPD 7: G(22)(i)	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: CP-10(1).1		

Assessment Objective

Determine if the organization includes a full recovery and reconstitution of the information system 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 test procedures; contingency plan test results; other relevant documents or records.

Interview: Organizational personnel with information system recovery and reconstitution responsibilities; organizational personnel with contingency testing responsibilities.

Identification and Authentication (IA) – *Technical*

IA-1 – Identification and Authentication Policy and Procedures (High)

Control

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

Guidance

The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and SP 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**Reference(s):** ARS: IA-1; FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.3.1#1.1; PISP: 4.7.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents identification and authentication policy and procedures;

(ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review identification and authentication policy and procedures;

(iv) the organization updates identification and authentication policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.

Interview: Organizational personnel with identification and authentication responsibilities.

ASSESSMENT PROCEDURE: IA-1.2

Assessment Objective

Determine if:
(i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated identification and authentication controls.

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 – User Identification and Authentication (High)

Control

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique IA of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

Implementation Standard(s)

1. Require the use of system and/or network authenticators and unique user identifiers.
2. All passwords shall be encrypted in transit and at rest.
3. Help desk support requires user identification for any transaction that has information security implications.

Guidance

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in SP 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST SP 800-63 level 1 compliant. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.
In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST SP 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals.

Applicability: All	**Reference(s):** ARS: IA-2; 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; PISP: 4.7.2	**Related Controls Requirement(s):** AC-14, AC-17, MA-4

ASSESSMENT PROCEDURE: IA-2.1

Assessment Objective

Determine if:
(i) the information system uniquely identifies and authenticates users (or processes acting on behalf of users);

(ii) authentication levels for users (or processes acting on behalf of users) are consistent with NIST Special Publication 800-63 and e-authentication risk assessment results.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system design documentation; e-authentication risk assessment results; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(1) – Enhancement (High)

Control

Not applicable.

Applicability: All	**Reference(s):** ARS: IA-2(1); HIPAA: 164.312(d); IRS-1075: 5.6.3.1#1.2	**Related Controls Requirement(s):**

IA-2(2) – Enhancement (High)

Control

Employ multifactor authentication for local system access that is at least NIST SP 800-63 level 3 compliant.

Applicability: All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC	**Reference(s):** ARS: IA-2(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-2(2).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the NIST Special Publication 800-63 authentication levels for the information system;

(ii) the information system employs multifactor authentication for local system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3 or level 4.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; System Security Plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-2(3) – Enhancement (High)

Control

Employ multifactor authentication for remote system access that is NIST SP 800-63 level 4 compliant.

Applicability: All	**Reference(s):** ARS: IA-2(3)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-2(3).1

Assessment Objective

Determine if:
(i) the organization defines the NIST Special Publication 800-63 authentication levels for the information system;

(ii) the information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 level 4 compliant.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-3 – Device Identification and Authentication (High)

Control

Automated mechanisms shall be used to enable IA of the CMS information system being used and to which a connection is being made before establishing a connection.

Implementation Standard(s)

1. Implement an information system that uses either a shared secret or digital certificate to identify and authenticate specific devices before establishing a connection.

Guidance

The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Applicability: All	**Reference(s):** ARS: IA-3; FISCAM: AC-1, AC-2; IRS-1075: 5.6.3.1#1.2; PISP: 4.7.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-3.1

Assessment Objective

Determine if:
(i) the organization defines the devices for which identification and authentication is required before establishing connections to the information system;

(ii) the information system uniquely identifies and authenticates the devices defined by the organization before establishing connections to the information system;

(iii) the information system employs device authentication mechanisms with strength of mechanism determined by the FIPS 199 security categorization of the information system.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; 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

Procedures shall be developed, documented, and implemented effectively to manage user identifiers. The procedures shall address processes and controls for:
4.7.4.1. Identifying each user uniquely;
4.7.4.2. Verifying the identity of each user;
4.7.4.3. Receiving authorization to issue a user identifier from an appropriate organization official;
4.7.4.4. Ensuring that the user identifier is issued to the intended party;
4.7.4.5. Disabling user identifier after a specific period of inactivity; and
4.7.4.6. Archiving user identifiers.

Reviews and validation of system users' accounts shall be conducted to ensure the continued need for access to a system. Identifier management shall not be applicable to shared information system accounts (i.e., guest and anonymous).

Implementation Standard(s)

1. Disable user identifiers after 90 days of inactivity and delete disabled accounts during annual re-certification process.
2. Require system administrator to maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.

Guidance

Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors.

Applicability: All	**Reference(s):** ARS: IA-4; FISCAM: AC-2, AC-3, AC-4, AS-2; IRS-1075: 5.6.3.1#2; PISP: 4.7.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-4.1

Assessment Objective

Determine if:
(i) the organization manages user identifiers by uniquely identifying each user;

(ii) the organization manages user identifiers by verifying the identity of each user;

(iii) the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official;

(iv) the organization manages user identifiers by issuing the identifier to the intended party;

(v) the organization defines in the System Security Plan, explicitly or by reference, the time period of inactivity after which a user identifier is to be disabled;

(vi) the organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity;

(vii) the organization manages user identifiers by archiving identifiers.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; System Security Plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

IA-5 – Authenticator Management (High)

Control

Procedures shall be developed, documented, and implemented effectively to manage user authenticators. The procedures shall address processes and controls for: initial authenticator content; distribution for new, lost, compromised, or damaged authenticators; revocation of authenticators; changing default authenticators; and changing / refreshing authenticators at specified intervals. Users shall not loan or share authenticators with other users. Lost or compromised authenticators shall be reported immediately to appropriate authority.

Selection of passwords or other authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS System Security Level of the information system. Automated mechanisms shall be in place for password-based authentication, to ensure that the information system:
4.7.5.1. Protects passwords from unauthorized disclosure and modification when stored and transmitted;
4.7.5.2. Prohibits passwords from being displayed when entered;
4.7.5.3. Enforces automatic expiration of passwords;
4.7.5.4. Prohibits password reuse for a specified number of generations; and
4.7.5.5. Enforces periodic password changes.

Implementation Standard(s)

1. For password-based authentication:
(a) Passwords are controlled by the assigned user and not subject to disclosure,
(b) The use of dictionary names or words as passwords is prohibited,
(c) When using passwords in connection with e-authentication, refer to ARS Appendix D: E-authentication Standard for further guidance,
(d) Force users to select a password comprising a minimum of eight (8) alphanumeric and special characters,
(e) Automatically force users (including administrators) to change user account passwords after sixty (60) days and system account passwords every 180 days,
(f) Enforce password lifetime restrictions within a minimum of one (1) day and maximum of sixty (60) days for user accounts and one hundred and eighty (180) days for system accounts, and
(g) Automatically force users to select six (6) unique passwords prior to reusing a previous one

Guidance

Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**Reference(s):** ARS: IA-5; FISCAM: AC-2, AS-2; IRS-1075: 5.6.3.1#2; PISP: 4.7.5	**Related Controls Requirement(s):** AC-11.Std.1, AC-CMS-1.Std.2

ASSESSMENT PROCEDURE: IA-5.1

Assessment Objective

Determine if:
(i) the organization manages information system authenticators by defining initial authenticator content;

(ii) the organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;

(iii) the organization manages information system authenticators by changing default authenticators upon information system installation;

(iv) the organization manages information system authenticators by changing/refreshing authenticators periodically.

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-6 – Authenticator Feedback (High)

Control

Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to obscure feedback to users during the authentication process to protect the information from possible exploitation / use by unauthorized individuals.

Implementation Standard(s)

1. Configure the information system to obscure passwords during the authentication process (e.g., display asterisks).

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):** ARS: IA-6; FISCAM: AC-2; IRS-1075: 5.6.3.1#1.2; PISP: 4.7.6	**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

Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Guidance

The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates FIPS 140-2 issued by the NIST Cryptographic

Module Validation Program remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	**Reference(s):** ARS: IA-7; FISCAM: AC-4; PISP: 4.7.7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-7.1

Assessment Objective

Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).

Assessment Methods And Objects

Examine: Identification and authentication policy; FIPS 140-2 (as amended); 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.

Incident Response (IR) – *Operational*

IR-1 – Incident Response Policy and Procedures (High)

Control

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed, documented, and implemented effectively to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-61 and current CMS Procedures.

Guidance

The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

Applicability: All	**Reference(s):** ARS: IR-1; FISCAM: AC-5, AS-1, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1; PISP: 4.8.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents incident response policy and procedures;
(ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review incident response policy and procedures;
(iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.

Interview: Organizational personnel with incident response responsibilities.

ASSESSMENT PROCEDURE: IR-1.2

Assessment Objective

Determine if:
(i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;
(iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated incident response controls.

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

All personnel shall be trained in their IR roles and responsibilities with respect to a CMS information system. Personnel shall receive periodic refresher training in IR procedures.

Implementation Standard(s)

1. Provide training on incident response roles and responsibilities of personnel every 365 days.

Guidance

Procedures and 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) 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):** ARS: IR-2; FISCAM: AC-5; IRS-1075: 5.6.2.6#2.1-2; PISP: 4.8.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-2.1

Assessment Objective

Determine if:
(i) the organization identifies and documents personnel with incident response roles and responsibilities;
(ii) the organization provides incident response training to personnel with incident response roles and responsibilities;
(iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;
(iv) the organization defines in the System Security Plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually;
(v) 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; System Security 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

Incorporate simulated events as part of incident response training.

Applicability: All	**Reference(s):** ARS: IR-2(1)	**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

Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

Applicability: All	**Reference(s):** ARS: IR-2(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-2(2).1

Assessment Objective

Determine if the organization employs automated incident response training mechanisms to provide a more thorough and realistic 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 IR capability for a CMS information system shall be tested periodically using appropriate tests, procedures, automated mechanisms, and exercises to determine the plan's effectiveness. The test results, procedures, and exercises employed to conduct the test shall be documented.

Implementation Standard(s)

1. Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations.

Guidance

NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Applicability: All	**Reference(s):** ARS: IR-3; FISCAM: AC-5; IRS-1075: 5.6.2.6#2.1-2; PISP: 4.8.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-3.1

Assessment Objective

Determine if:

(i) the organization defines in the System Security Plan, explicitly or by reference, incident response tests/exercises;

(ii) the organization defines in the System Security Plan, explicitly or by reference, the frequency of incident response tests/exercises and the frequency is at least annually;

(iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;

(iv) the organization documents the results of incident response tests/exercises;

(v) 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; System Security Plan; incident response testing material; incident response test results; other relevant documents or records.

IR-3(1) – Enhancement (High)

Control

Employ automated mechanisms to test / exercise the incident response plan.

Guidance

Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the 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):** ARS: IR-3(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-3(1).1

Assessment Objective

Determine if:
(i) the organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability for the information system;

(ii) the automated mechanisms supporting incident response testing provide more complete coverage of incident response issues, more realistic test/exercise scenarios, and a greater stress on the incident response capability.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response testing and exercises; System Security Plan; incident response testing documentation; automated mechanisms supporting incident response tests/exercises; other relevant documents or records.

Interview: Organizational personnel with incident response testing responsibilities.

IR-4 – Incident Handling (High)

Control

An incident handling capability, which includes preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents, shall be established and maintained. Evidence of computer crimes, computer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learned from on-going incident handling activities shall be incorporated into the IR procedures.

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. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.

Applicability: All	**Reference(s):** ARS: IR-4; FISCAM: AC-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; PISP: 4.8.4	**Related Controls Requirement(s):** AU-6, PE-6, SI-2

ASSESSMENT PROCEDURE: IR-4.1		
Assessment Objective Determine if: (i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; (ii) the organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. **Assessment Methods And Objects** **Examine:** Incident response policy; procedures addressing incident handling; NIST Special Publication 800-61; other relevant documents or records. **Interview:** Organizational personnel with incident handling responsibilities. **Test:** Incident handling capability for the organization.		
IR-4(1) – Enhancement (High)		
Control Employ automated mechanisms to support the incident handling process.		
Applicability: All	**Reference(s):** ARS: IR-4(1); 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 On-going monitoring of the CMS information system for security events shall be conducted. All events and activities associated with system performance shall be monitored for the identification of resources used by processes and user activity that may indicate security threats resulting from user, software, or hardware activity. All information system security incidents shall be tracked and documented on an on-going basis. All user activities shall be subject to monitoring to verify compliance with this policy and to detect actions that may be in violation of this policy.		
Guidance It is good practice to separate system performance issues from incident tracking. However, unexplained system performance changes can be the result of a security incident occurring or data corruption in transmission within the system. Checksums or cyclic redundancy checks (CRCs) can help during the investigation of these problems. While useful for error detection, CRCs cannot be safely relied upon to fully verify data correctness in the face of deliberate (rather than random) changes. Remote Procedure Calls (RPCs) can cause performance/incident issues. Note: If an attacker (internal or external person) is able to successfully exploit an RPC vulnerability they could gain complete control over a remote computer. This would give the attacker the ability to take any action on the system that they want. For example, an attacker could change web pages, reformat the hard disk, and / or add new users to the local administrators group. Performance and incident tracking on an on-going basis can denote trends within the system or network architecture.		
Applicability: All	**Reference(s):** ARS: IR-5; FISCAM: AC-5, SM-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#2.3; PISP: 4.8.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-5.1

Assessment Objective

Determine if the organization tracks and documents information system security incidents on an ongoing basis.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; 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

Employ automated mechanisms to assist in tracking and analyzing security incidents.

Applicability: All	**Reference(s):** ARS: IR-5(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-5(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident monitoring; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting incident monitoring; other relevant documents or records.

Interview: Organizational personnel with incident monitoring responsibilities.

Test: Automated mechanisms assisting in tracking of security incidents and in the collection and analysis of incident information.

IR-6 – Incident Reporting (High)

Control

All IS incidents, or suspected incidents, shall be reported to the CMS IT Service Desk (or equivalent organizational function) as soon as an incident comes to the attention of a user of CMS information or information systems. Events and confirmed security incidents by business partners shall also be reported to the CMS IT Service Desk in accordance with established procedures.

Guidance

The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST SP 800-61 provides guidance on incident reporting.

Applicability: All	**Reference(s):** ARS: IR-6; FISCAM: AC-5; PISP: 4.8.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-6.1

Assessment Objective

Determine if:
(i) the organization promptly reports incident information to appropriate authorities;
(ii) incident reporting is consistent with NIST Special Publication 800-61;

(iii) the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance;

(iv) weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident reporting; NIST Special Publication 800-61; incident reporting records and documentation; other relevant documents or records.

Interview: Organizational personnel with incident reporting responsibilities.

IR-6(1) – Enhancement (High)

Control

Employ automated mechanisms to assist in the reporting of security incidents.

Applicability: All	**Reference(s):** ARS: IR-6(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-6(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; other relevant documents or records.

Interview: Organizational personnel with incident reporting responsibilities.

IR-7 – Incident Response Assistance (High)

Control

A CMS IT Service Desk (or equivalent organizational function) shall be in place and shall play an appropriate role in the organization's IR program. The CMS IT Service Desk shall offer advice to users of a CMS information system. Procedures shall be developed, documented, and implemented effectively to facilitate the incident response by providing central incident support resource for CMS information system users.

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.

Applicability: All	**Reference(s):** ARS: IR-7; FISCAM: AC-5; PISP: 4.8.7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-7.1

Assessment Objective

Determine if:
(i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents;

(ii) the incident response support resource is an integral part of the organization's incident response capability.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; other relevant documents or records.

Interview: Organizational personnel with incident response assistance and support responsibilities.

IR-7(1) – Enhancement (High)		
Control Employ automated mechanisms to increase the availability of incident response-related information and support.		
Applicability: All	**Reference(s):** ARS: IR-7(1)	**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 for incident response support. **Assessment Methods And Objects** **Examine:** Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; other relevant documents or records. **Interview:** Organizational personnel with incident response support and assistance responsibilities and organizational personnel that require incident response support and assistance.		

Maintenance (MA) – *Operational*

MA-1 – System Maintenance Policy and Procedures (High)

Control

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

Guidance

The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: MA-1; 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; PISP: 4.9.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents information system maintenance policy and procedures;

(ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review information system maintenance policy and procedures;

(iv) the organization updates information system maintenance policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

ASSESSMENT PROCEDURE: MA-1.2

Assessment Objective

Determine if:
(i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated system maintenance controls.

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

Comprehensive maintenance procedures shall be developed, documented, and implemented effectively to conduct controlled periodic on-site and off-site maintenance of the

CMS information systems and of the physical plant within which these information systems reside. 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.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS-approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly.

Implementation Standard(s)

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

All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Applicability: All; Optional for SS	**Reference(s):** ARS: MA-2; 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; PISP: 4.9.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-2.1

Assessment Objective

Determine if the organization schedules, performs, documents, and reviews 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.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-2(1) – Enhancement (High)

Control

Maintain maintenance records for each information system that includes:
(a) Date and time of maintenance,
(b) Name of the individual performing the maintenance, name of escort, if applicable,
(c) Description of the maintenance performed, and
(d) List of equipment removed or replaced (including identification numbers, if applicable).

Applicability: All; Optional for SS	**Reference(s):** ARS: MA-2(1)	**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: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; (v) a 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

Employ automated mechanisms to ensure that maintenance is scheduled and conducted as required, and that a record of maintenance actions, both needed and complete, is up-to-date, accurate, and readily available.

Applicability: All	**Reference(s):** ARS: MA-2(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-2(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to schedule and conduct maintenance as required, and to create accurate, complete, and available records of all maintenance actions, both needed and completed.

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

The use of system maintenance tools, including diagnostic and test equipment and administration utilities, shall be approved, controlled, and monitored. Approved tools shall be maintained on an on-going basis.

Guidance

The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/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):** ARS: MA-3; FISCAM: AC-4, CP-2; IRS-1075: 5.6.2.4#1.2, 5.6.2.4#1.3; PISP: 4.9.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-3.1

Assessment Objective

Determine if:
(i) the organization approves, controls, and monitors the use of information system maintenance tools;
(ii) the organization maintains 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(1) – Enhancement (High)

Control

Inspect all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.

Guidance

Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

Applicability: All	**Reference(s):** ARS: MA-3(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-3(1).1

Assessment Objective

Determine if the organization inspects all maintenance tools (e.g., diagnostic and test equipment) 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

Check all media containing diagnostic and test programs for malicious code before the media is used in the system.

Applicability: All	**Reference(s):** ARS: MA-3(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-3(2).1

Assessment Objective

Determine if the organization checks all media containing diagnostic 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

Check all maintenance equipment with the capability of retaining information to ensure that no sensitive information is saved on the equipment and that the equipment is appropriately sanitized prior to release. If the equipment cannot be sanitized, the equipment must remain within the facility or be destroyed, unless an exception is specifically authorized.

Applicability: All	**Reference(s):** ARS: MA-3(3)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-3(3).1

Assessment Objective

Determine if the organization either (a) checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; or (b) retains the maintenance equipment within the facility or destroys the equipment if the equipment cannot be sanitized, unless an appropriate organization official explicitly authorizes an exception.

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-3(4) – Enhancement (High)

Control

Employ automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

Applicability: All	**Reference(s):** ARS: MA-3(4)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-3(4).1

Assessment Objective

Determine if the organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; automated mechanisms supporting information system maintenance activities; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

Test: Automated mechanisms supporting information system maintenance activities.

MA-4 – Remote Maintenance (High)

Control

Remote maintenance of a CMS information system must be approved by the CIO or his/her designated representative. Remote maintenance procedures shall be developed, documented, and implemented effectively to provide additional controls on remotely executed maintenance and diagnostic activities.

The use of remote diagnostic tools shall be described in the SSP for the information system. Maintenance records for all remote maintenance, diagnostic, and service activities shall be maintained and shall be reviewed periodically by appropriate organization officials. All sessions and remote connections shall be terminated after the remote maintenance is completed. If password-based authentication is used during remote maintenance, the passwords shall be changed following each remote maintenance service.

Implementation Standard(s)

1. If remote maintenance is authorized in writing by the CIO or his/her designated representative:
Encrypt and decrypt diagnostic communications; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, terminate all sessions and remote connections. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.

Guidance

Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST SP 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Applicability: All	**Reference(s):** ARS: MA-4; 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; PISP: 4.9.4	**Related Controls Requirement(s):** IA-2, MP-6

ASSESSMENT PROCEDURE: MA-4.1

Assessment Objective

Determine if:
(i) the organization authorizes, monitors, and controls the execution of maintenance and diagnostic activities conducted remotely by individuals communicating through an external, non-organization-controlled network (e.g., the Internet), if employed;

(ii) the organization documents in the System Security Plan, the remote maintenance and diagnostic tools to be employed;

(iii) the organization maintains records for all remote maintenance and diagnostic activities;

(iv) the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of remote maintenance and diagnostic activity when the remote maintenance or diagnostics is completed;

(v) the organization changes the passwords following each remote maintenance and diagnostic activity if password-based authentication is used to accomplish remote maintenance.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; 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

Audit all remote maintenance sessions, and ensure that appropriate information security personnel review the maintenance records of the remote sessions.

Applicability: All	**Reference(s):** ARS: MA-4(1); 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:
(i) the organization audits all remote maintenance and diagnostic sessions;

(ii) appropriate organizational personnel (as deemed by the organization) review the maintenance records of remote sessions.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote 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

Document the use of remote diagnostic tools in the SSP.

Applicability: All	**Reference(s):** ARS: MA-4(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-4(2).1

Assessment Objective

Determine if the organization addresses the installation and use of remote maintenance and diagnostic links in the System Security Plan.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; System Security Plan; maintenance records; audit records; other relevant documents or records.

MA-4(3) – Enhancement (High)

Control

Require that remote diagnostic or maintenance service organizations utilize the same level of security as the CMS system being serviced. If the service organization does not use at least the same level of security, maintenance is prohibited unless the component being serviced is removed from the information system and sanitized (with regard to CMS sensitive information) before the service begins. The component is also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system. If the system cannot be sanitized (e.g., due to a system failure), remote maintenance is not permitted.

Applicability: All	**Reference(s):** ARS: MA-4(3)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-4(3).1

Assessment Objective

Determine if the organization does not allow remote diagnostic or maintenance services to be performed by a provider that does not implement for its own information system, a level of security at least as high as the level of security implemented on the information system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing remote 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

Maintenance personnel procedures shall be developed, documented, and implemented effectively to control maintenance of CMS information systems. A list of individuals authorized to perform maintenance on the information system shall be maintained.

Implementation Standard(s)

1. Only authorized individuals are allowed to perform maintenance. Ensure maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. Supervise maintenance personnel during the performance of maintenance activities when they do not have the needed access authorizations.

Guidance

Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Applicability: All	**Reference(s):** ARS: MA-5; FISCAM: CP-2, SM-7; PISP: 4.9.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-5.1

Assessment Objective

Determine if:
(i) the organization allows only authorized personnel to perform maintenance on the information system;
(ii) the organization supervises authorized maintenance personnel who do not have needed access authorizations to the information system during the performance of

maintenance activities on the system using organizational personnel with appropriate access authorizations.

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; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-6 – Timely Maintenance (High)

Control

Maintenance services and parts shall be available in a timely manner.

Implementation Standard(s)

1. Obtain maintenance support and 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

It is good practice to determine the priority of each system based on the criticality of the system for continued business operations. Each system should be prioritized and interconnections between each of the enterprise's systems mapped and dataflow diagrams developed.
Next maintenance contracts as well as emergency maintenance considerations will determine needed availability and pre-placement of spare parts.

Applicability: All	**Reference(s):** ARS: MA-6; FISCAM: CP-2; PISP: 4.9.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-6.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, key information system components;

(ii) the organization defines in the System Security Plan, explicitly or by reference, the time period within which support and spare parts must be obtained after a failure;

(iii) the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period 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; System Security Plan; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-CMS-1 – Off-site Physical Repair of Systems (High)

Control

Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality.

Implementation Standard(s)

1. Access to system for repair must be by authorized personnel only. Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After maintenance is performed, check security features to verify they are functioning properly.

Guidance

It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approved Change Management baseline.
Storage media control when encrypted may take special considerations.

Applicability: All	**Reference(s):** ARS: MA-CMS-1; PISP: 4.9.7	**Related Controls Requirement(s):** AC-

		19.Std.1, AC-3, CP-9, SC-12.Std.1

ASSESSMENT PROCEDURE: MA-CMS-1.1

Assessment Objective

Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair.

Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.

MA-CMS-2 – On-site Physical Repair of Systems (High)

Control

Controls shall be developed, documented, and implemented effectively to enable on-site physical repair of systems without compromising security functionality or confidentiality.

Implementation Standard(s)

1. Access to system for repair must be by authorized personnel only.
2. Physical repair of servers must be within protected environments.

Guidance

It is good practice to complete a full security review of a system before it is put back into operation when the system has completed repairs. The repaired system should match the approved Change Management baseline.
Storage media control when encrypted may take special considerations.

Applicability: All	**Reference(s):** ARS: MA-CMS-2; PISP: 4.9.8	**Related Controls Requirement(s):** AC-19.Std.1, AC-3, CP-9, SC-12.Std.1

ASSESSMENT PROCEDURE: MA-CMS-2.1

Assessment Objective

Determine if the organization effectively develops procedures, documents procedures, and implements on-site repair of systems without compromising security functionality or confidentiality.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for on-site repair.

Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during on-site repair.

Media Protection (MP) – *Operational*

MP-1 – Media Protection Policy and Procedures (High)

Control

MP controls and procedures shall be developed, documented, and implemented effectively to address media access; media labeling; media transport; media destruction; media sanitization and clearing; media storage; and disposition of media records. The MP procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Implementation Standard(s)

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

The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: MP-1; FISCAM: AC-6, AS-1, SM-1, SM-3; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1; PISP: 4.10.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MP-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents media protection policy and procedures;

(ii) the organization disseminates media protection policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review media protection policy and procedures;

(iv) the organization updates media protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system media protection responsibilities.

ASSESSMENT PROCEDURE: MP-1.2

Assessment Objective

Determine if:
(i) the media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated media protection controls.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system media protection responsibilities.

MP-2 – Media Access (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media based on the sensitivity of the CMS information. Automated mechanisms shall be implemented to control access to media storage areas and to audit access attempts and access granted.

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 portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).
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. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Applicability: All	**Reference(s):** ARS: MP-2; 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; PISP: 4.10.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MP-2.1

Assessment Objective

Determine if the organization restricts access to information system media to authorized users.

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

Employ automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Guidance

This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

Applicability: All	**Reference(s):** ARS: MP-2(1); IRS-1075: 4.6#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MP-2(1).1

Assessment Objective

Determine if:
(i) the organization employs automated mechanisms to restrict access to media storage areas;

(ii) the organization employs automated mechanisms to audit access attempts and access granted.

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 devices; access control records; audit records; other relevant documents or records.

Test: Automated mechanisms implementing access restrictions to media storage areas.

MP-3 – Media Labeling (High)

Control

Storage media and information system output shall have external labels affixed to indicate the distribution limitations, applicable security classification, and handling caveats of the information. Specific types of media or hardware components may be exempted from the labeling requirement, so long as the exempted items remain within a secure environment. Only the CIO or his/her designated representative shall have the authority to exempt specific types of media or hardware components from the labeling requirement.

Implementation Standard(s)

1. Off-line backup storage media must be marked according to backup rotation schedule for ease of retrieval.

Guidance

An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Applicability: All	**Reference(s):** ARS: MP-3; FISCAM: AC-4; IRS-1075: 4.6#1, 5.1#1.2, 5.3#2.1-2, 5.3#3; PISP: 4.10.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MP-3.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, its protected environment for media labeling requirements;

(ii) the organization defines in the System Security Plan, explicitly or by reference, media types and hardware components that are exempted from external labeling requirements;

(iii) the organization affixes external labels to removable information storage media and information system output not otherwise exempted from this labeling requirement, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; System Security Plan; removable storage media and information system output; other relevant documents or records.

MP-4 – Media Storage (High)

Control

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper, within controlled areas. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security level of the information ever recorded on it until destroyed or sanitized using CMS-approved procedures.

Implementation Standard(s)

1. (For PII only) Evaluate employing an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest, consistent with NIST SP 800-66 guidance.
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

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). 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 the information and/or information system. This control applies to portable and mobile computing and

communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). 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 exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management.

Applicability: All	**Reference(s):** ARS: MP-4; FISCAM: AC-4, AC-6; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1; PISP: 4.10.4	**Related Controls Requirement(s):** AC-19, CP-9, CP-9(4), RA-2, SC-7

ASSESSMENT PROCEDURE: MP-4.1

Assessment Objective

Determine if:

(i) the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk;

(ii) the organization defines the specific measures used to protect the selected media and information contained on that media;

(iii) the organization physically controls and securely stores information system media within controlled areas;

(iv) the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; System Security Plan; information system media; other relevant documents or records.

MP-5 – Media Transport (High)

Control

Physical, administrative, and technical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) to authorized personnel based on the sensitivity of the CMS information.

Implementation Standard(s)

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.
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, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). 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 the information and/or information system. This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) 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 exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Applicability: All	**Reference(s):** ARS: MP-5; FISCAM: AC-4; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.6#2, 4.6#4; PISP: 4.10.5	**Related Controls Requirement(s):** AC-19, CP-9, CP-9(4)

ASSESSMENT PROCEDURE: MP-5.1

Assessment Objective

Determine if:
(i) the organization identifies personnel authorized to transport information system media outside of controlled areas;

(ii) the organization documents, in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media;

(iii) the organization protects and controls information system media during transport outside of controlled areas;

(iv) the organization restricts the activities associated with transport of information system media to authorized personnel.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; System Security Plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records.

MP-5(1) – Enhancement (High)

Control

All sensitive information stored on digital media are protected during transport outside of controlled areas by 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.
If the use of cryptography is not technically feasible or the sensitive information is stored on non-digital media, written management approval (one level below the CIO) must be obtained prior to transport and the information must be (a) hand carried using securable container via authorized personnel, or (b) if shipped, by United States Postal Service (USPS) Certified Mail with return receipt in tamper-evident packaging.
Correspondence pertaining to a single individual may be mailed through regular USPS mail, but should contain only the minimal amount of sensitive information in order to reduce the risk of unauthorized disclosure (e.g., partially masking social security numbers).

Guidance

Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used.

Applicability: All	**Reference(s):** ARS: MP-5(1); HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MP-5(1).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, security measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas;

(ii) the organization protects digital and non-digital media during transport outside of controlled areas using the organization-defined security measures.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; System Security Plan; information system media transport records; audit records; other relevant documents or records.

Interview: Organizational personnel with information system media transport responsibilities.

MP-5(2) – Enhancement (High)

Control

Activities associated with the transport of sensitive information system media are documented.

Guidance

Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

Applicability: All	**Reference(s):** ARS: MP-5(2); 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:
(i) the organization defines in the System Security Plan, explicitly or by reference, a system of records for documenting activities associated with the transport of information system media;

(ii) the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; System Security Plan; information system media transport records; audit records; other relevant documents or records.

MP-5(3) – Enhancement (High)

Control

Employ an identified custodian at all times to transport information system media.

Guidance

Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

Applicability: All	**Reference(s):** ARS: MP-5(3); 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 at all times to transport 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-6 – Media Sanitization and Disposal (High)

Control

Formal documented procedures shall be developed and implemented effectively to ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of data residing on storage devices, equipment, and hard copy documents. Media sanitization actions shall be tracked, documented, and verified. Sanitization equipment and procedures shall be tested periodically to ensure proper functionality.

Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmentally approved manner, to facilitate the disposal of media, both electronic and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. Approved equipment removal procedures for CMS information systems and components that have processed or contained CMS information shall be followed. Inventory and disposition records for media, both electronic and paper, shall be produced, stored, updated, and retained.

Implementation Standard(s)

1. The sanitization process includes the removal of all data, labels, marking, and activity records using NSA Guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, Guidelines for Media Sanitization.
2. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.
3. (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.
4. (For PII only) Authorized employees of the recipient 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

Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on 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 the organization or individuals if released for reuse or disposed. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Applicability: All	**Reference(s):** ARS: MP-6; 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; PISP: 4.10.6	**Related Controls Requirement(s):** MA-4

ASSESSMENT PROCEDURE: MP-6.1

Assessment Objective

Determine if:
(i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process;

(ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse;

(iii) information system media sanitation is consistent with NIST Special Publication 800-88.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST Special Publication 800-88; media sanitization records; 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

It is good practice for, electronic, inventory records maintenance that a hash function (a reproducible method of turning inventory data into a (relatively) small number that may serve as a digital "fingerprint" of the data) be performed periodically so that 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):** ARS: MP-CMS-1; FISCAM: AC-6; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4; PISP: 4.10.7	**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.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information.

Interview: Organizational personnel with information system media protection responsibilities to determine inventory and disposition records are maintained for information system media to ensure control and accountability of CMS information.

Physical and Environmental Protection (PE) – *Operational*

PE-1 – Physical and Environmental Protection Policy and Procedures (High)

Control

Physical and environmental protection procedures shall be developed and implemented effectively to protect all CMS IT infrastructure and assets from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional. These procedures shall meet all federal, state and local building codes and be consistent with General Services Administration policies, directives, regulations, and guidelines.

Guidance

The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: PE-1; 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; PISP: 4.11.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents physical and environmental protection policy and procedures;

(ii) the organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review physical and environmental protection policy and procedures;

(iv) the organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required.

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.

ASSESSMENT PROCEDURE: PE-1.2

Assessment Objective

Determine if:
(i) the physical and environmental protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated physical and environmental protection controls.

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

Access lists of personnel with authorized access to facilities containing CMS information or information systems (except for those areas within the facilities officially designated as publicly accessible) shall be documented on standard forms, maintained on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessary, updated. Appropriate authorization credentials (e.g., badges, identification cards, smart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be removed promptly from all access lists.

Implementation Standard(s)

1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every 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

Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides.

Applicability: All	**Reference(s):** ARS: PE-2; FISCAM: AC-6; PISP: 4.11.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-2.1

Assessment Objective

Determine if:
(i) the organization identifies areas within the facility that are publicly accessible;

(ii) the organization defines in the System Security Plan, explicitly or by reference, the frequency of review and approval for the physical access list and authorization credentials for the facility and the frequency is at least annually;

(iii) 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);

(iv) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards);

(v) designated officials within the organization review and approve the access list and authorization credentials in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records.

PE-3 – Physical Access Control (High)

Control

Physical access control devices (e.g., keys, locks, combinations, card-readers) and/or guards shall be used to control entry to and exit from facilities containing CMS information or information systems, except for areas and/or facilities officially designated as publicly accessible. Individual access authorizations shall be verified before granting access to facilities containing CMS information or information systems. Physical access control devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis.

Combinations, access codes, and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry to facilities during emergency-related events shall be restricted to authorized individuals only. Access to workstations and associated peripheral computing devices shall be appropriately controlled when located in areas designated as publicly accessible.

Implementation Standard(s)

1. Control data center / facility access by use of door and window locks, and security staff or physical authentication devices, such as biometrics and/or smart card / PIN combination.
2. Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.

3. Restrict access to grounds / facilities to authorized persons only.
4. Controls are established to protect access authorization lists to secure areas such as data centers.
5. (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

The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST SP 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST SP 800-76.

Applicability: All	**Reference(s):** ARS: PE-3; FISCAM: AC-6, SD-1, SM-4; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1; PISP: 4.11.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-3.1

Assessment Objective

Determine if:
(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

(ii) the organization verifies individual access authorizations before granting access to the facility;

(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records.

Interview: Organizational personnel with physical access control responsibilities.

Test: Physical access control capability.

ASSESSMENT PROCEDURE: PE-3.2

Assessment Objective

Determine if:
(i) the organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems;

(ii) the organization secures and regularly inventories keys, combinations, and other access devices;

(iii) the organization changes combinations and keys periodically and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records.

Test: Physical access control devices.

ASSESSMENT PROCEDURE: PE-3.3

Assessment Objective

Determine if:

(i) the access control system is consistent with FIPS 201 and NIST Special Publication 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed);

(ii) the access control system is consistent with NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification);

(iii) the access control system is consistent with NIST Special Publication 800-76 (where the token-based access control function employs biometric verification).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records.

PE-3(1) – Enhancement (High)

Control

Physical access control to the information system is independent of the physical access controls for the facility.

Guidance

This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.

Applicability: All	**Reference(s):** ARS: PE-3(1); IRS-1075: 4.6#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-3(1).1

Assessment Objective

Determine if:
(i) the organization identifies specific areas within the facility that, due to the concentration of information system components or the impact level of the components, require additional physical protections over those afforded to the facility as a whole;

(ii) for an information system identified as requiring additional physical protection or part of a large concentration of information system components, the organization controls physical access to the 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

Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering of CMS information system transmission lines within organizational facilities that carry unencrypted information.

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):** ARS: PE-4; FISCAM: AC-6; PISP: 4.11.4	**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.

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 Display Medium (High)

Control

Physical access controls shall be developed, documented, and implemented effectively to prevent unauthorized individuals from observing CMS sensitive information displayed on information system devices.

Guidance

It is good practice to position sensitive information display devices away from windows and areas of ingress and egress.

Applicability: All	**Reference(s):** ARS: PE-5; FISCAM: AC-6; HIPAA: 164.310(b); PISP: 4.11.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-5.1

Assessment Objective

Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display 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

Physical access to information systems shall be monitored for physical security compliance and to detect and respond to incidents. Appropriate organization officials shall periodically review physical access records, investigate apparent security violations or suspicious physical access activities, and take appropriate remedial action.

Guidance

The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.

Applicability: All	**Reference(s):** ARS: PE-6; FISCAM: AC-5, AC-6, SM-5; PISP: 4.11.6	**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.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; other relevant documents or records.

Interview: Organizational personnel with physical access monitoring responsibilities.

Test: Physical access monitoring capability.

PE-6(1) – Enhancement (High)

Control

Monitor real-time physical intrusion alarms and surveillance equipment.

Applicability: All	**Reference(s):** ARS: PE-6(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-6(1).1

Assessment Objective

Determine if the organization monitors real-time intrusion alarms and surveillance equipment.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; intrusion alarm/surveillance equipment logs or records; other relevant documents or records.

Interview: Organizational personnel with physical access monitoring responsibilities.

Test: Physical access monitoring capability.

PE-6(2) – Enhancement (High)

Control

Automated mechanisms are implemented to recognize potential intrusions and initiate appropriate response actions.

Applicability: All	**Reference(s):** ARS: PE-6(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-6(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; information system design documentation; other relevant documents or records.

Test: Automated mechanisms implementing physical access monitoring capability.

PE-7 – Visitor Control (High)

Control

Visitor controls shall be developed, documented, and implemented effectively to control access to sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries. Visitors shall be authenticated prior to being granted access to facilities or areas other than areas designated as publicly accessible. Government contractors and others with permanent authorization credentials are not considered visitors.

Guidance

Government contractors and others with permanent authorization credentials are not considered visitors. CMS Personal Identity Verification (PIV) credentials for federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST SP 800-79. If PIV credentials are issued, they shall conform to FIPS 201.

Applicability: All	**Reference(s):** ARS: PE-7; FISCAM: AC-6; HIPAA: 164.310(a)(2)(iii); PISP: 4.11.7	**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.

Test: Visitor access control capability.

PE-7(1) – Enhancement (High)

Control

Escort visitors and monitor visitor activity.

Applicability: All	**Reference(s):** ARS: PE-7(1); 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 (High)

Control

Visitor access to sensitive facilities and restricted / controlled areas that contain CMS information or information systems shall be logged. The visitor access record shall contain:
4.11.8.1. Name and organization of the person visiting;
4.11.8.2. Signature of the visitor;
4.11.8.3. Form of identification;
4.11.8.4. Date of access;
4.11.8.5. Time of entry and departure;
4.11.8.6. Purpose of visit; and
4.11.8.7. Name and organization of person visited.

Appropriate organization officials shall periodically review the access records, including after closeout.

Implementation Standard(s)

1. Visitor access records must be closed out and reviewed by management monthly.

Guidance

It is good practice to have a standard log format for consistency and ease of use during log closeouts and the next months log generation.

Applicability: All	**Reference(s):** ARS: PE-8; FISCAM: AC-6; PISP: 4.11.8	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-8.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of review for visitor access records;

(ii) 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) that includes:
- name and organization of the person visiting;
- signature of the visitor;
- form of identification;
- date of access;
- time of entry and departure;
- purpose of visit;
- name and organization of person visited and

(iii) designated officials within the organization review the visitor access logs in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; System Security Plan; facility access control records; other relevant documents or records.

PE-8(1) – Enhancement (High)

Control

Employ automated mechanisms to facilitate the maintenance and review of access records.

Applicability: All	**Reference(s):** ARS: PE-8(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-8(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to facilitate the maintenance and review of access records.

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

Maintain records of all physical access, both visitor and authorized individuals.

Applicability: All	**Reference(s):** ARS: PE-8(2)	**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

Power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain safe power for CMS information systems.

Implementation Standard(s)

1. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.
2. Power surge protection must be implemented for all computer equipment.

Guidance

Both primary and backup power systems should be included in the safe power implementation procedures. Remote backup site's power implementation should be included in the documentation.

Applicability: All	**Reference(s):** ARS: PE-9; FISCAM: AC-6, CP-2; PISP: 4.11.9	**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.

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-9(1) – Enhancement (High)

Control

Employ redundant and parallel power cabling paths.

Applicability: All	**Reference(s):** ARS: PE-9(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-9(1).1

Assessment Objective

Determine if the organization employs redundant and parallel power cabling paths.

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

Emergency shut-off controls shall be developed, documented, and implemented effectively to provide the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

Implementation Standard(s)

1. Implement and maintain a master power switch or emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms.

Guidance

Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Applicability: All	Reference(s): ARS: PE-10; FISCAM: CP-2; PISP: 4.11.10	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: PE-10.1

Assessment Objective

Determine if:
(i) the organization identifies the specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms);
(ii) the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records.

PE-10(1) – Enhancement (High)

Control

Employ appropriate measures to protect the emergency power-off capability from accidental and intentional / unauthorized activation.

Applicability: All	Reference(s): ARS: PE-10(1)	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: PE-10(1).1

Assessment Objective

Determine if the organization protects the emergency power-off capability from accidental or unauthorized activation.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records.

PE-11 – Emergency Power (High)

Control

Emergency power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to facilitate an orderly shutdown of the CMS information system in the event of a primary power source loss.

Guidance

Both primary and backup processing locations should be included in the safe power implementation procedures. The remote backup site's power implementation should be included in the documentation. Even though unlikely that both the primary and backup locations will be switching to emergency power at the same time, it is prudent to minimize the risk to a total lose of a processing capability.

Applicability: All	Reference(s): ARS: PE-11; FISCAM: AC-6, CP-2; PISP: 4.11.11	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; other relevant documents or records.

Test: Uninterruptible power supply.

PE-11(1) – Enhancement (High)

Control

Provide a long-term alternate power supply for the 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):** ARS: PE-11(1)	**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

Mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enhance safety and availability. Automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes shall be provided.

Guidance

Local building safety codes are a good place to obtain the needed information for documenting emergency lighting implementation procedures and architecture.

Applicability: All	**Reference(s):** ARS: PE-12; FISCAM: AC-6, CP-2; PISP: 4.11.12	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-12.1

Assessment Objective

Determine if:
(i) the organization employs automatic emergency lighting that activates in the event of a power outage or disruption;
(ii) the organization employs automatic emergency lighting that covers emergency exits and evacuation routes;
(iii) the organization maintains the automatic emergency lighting.

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

Fire protection mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to prevent, detect, and respond to fire. Fire suppression and detection devices / systems that can be activated in the event of a fire shall be employed and maintained. Fire suppression and detection devices / systems shall include, but not be limited to, sprinkler systems, hand-held fire extinguishers, fixed fire hoses, and smoke detectors.

Guidance

Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Applicability: All	**Reference(s):** ARS: PE-13; FISCAM: CP-2; PISP: 4.11.13	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-13.1

Assessment Objective

Determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

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

Implement and maintain fire detection devices / systems that activate automatically and notify the organization and emergency responders in the event of a fire.

Applicability: All	**Reference(s):** ARS: PE-13(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-13(1).1

Assessment Objective

Determine if the organization employs fire detection devices/systems that, without manual intervention, 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 fire detection and automated notifications.

PE-13(2) – Enhancement (High)

Control

Employ fire suppression devices / systems that provide automatic notification of any activation to the organization and emergency responders.

Applicability: All	**Reference(s):** ARS: PE-13(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-13(2).1

Assessment Objective

Determine if the organization employs fire suppression devices/systems 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

Employ an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

Applicability: All	**Reference(s):** ARS: PE-13(3)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-13(3).1

Assessment Objective

Determine if the organization employs an automatic fire suppression capability in facilities that are 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

Temperature and humidity control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain (within acceptable levels) and monitor the temperature and humidity of facilities containing CMS information systems.

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

Local building a safety codes are a good place to obtain the needed information for documenting HVAC implementation procedures and architecture. Consideration for Occupational Safety and Health Administration (OSHA) requirements maybe included.

Applicability: All	**Reference(s):** ARS: PE-14; FISCAM: AC-6, CP-2; PISP: 4.11.14	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-14.1

Assessment Objective

Determine if:
(i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides;
(ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records.

PE-15 – Water Damage Protection (High)

Control

All necessary steps shall be taken to ensure that the building plumbing does not endanger CMS information systems. Procedures shall be developed, documented, and implemented effectively to reduce the potential damage from plumbing leaks.

Guidance

Local building a safety codes are a good place to obtain the needed information for documenting water damage protection procedures and architecture. Consideration for Occupational Safety and Health Administration (OSHA) requirements maybe included.

Applicability: All	**Reference(s):** ARS: PE-15; FISCAM: AC-6, CP-2; PISP: 4.11.15	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-15.1

Assessment Objective

Determine if:
(i) the organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible and working properly;

(ii) 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 values; list of key personnel with knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value 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

Mechanisms are employed that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.

Applicability: All	**Reference(s):** ARS: PE-15(1)	**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 significant 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

Procedures shall be developed, documented, and implemented effectively to control the flow of information system-related items into and out of the organization. Appropriate officials shall authorize the delivery or removal of CMS information system-related items.

To avoid unauthorized access, delivery and removal controls shall be implemented to isolate delivery areas from sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries.

Guidance

The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.

Applicability: All	Reference(s): ARS: PE-16; FISCAM: AC-6; PISP: 4.11.16	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: PE-16.1

Assessment Objective

Determine if:
(i) the organization authorizes and controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility;
(ii) the organization maintains appropriate records of items 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; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records.

Interview: Organization personnel with tracking responsibilities for information system components entering and exiting the facility.

Test: Process for controlling information system-related items entering and exiting the facility.

PE-17 – Alternate Work Site (High)

Control

Procedures shall be developed, documented, and implemented effectively to control information system security at alternate work sites. A method of communication shall be provided to employees at alternate work sites to report security issues or suspected security incidents.

Implementation Standard(s)

1. Employ appropriate security controls at alternate work sites. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

Guidance

The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST SP 800-46 provides guidance on security in telecommuting and broadband communications.

Applicability: All	Reference(s): ARS: PE-17; FISCAM: CP-2; HIPAA: 164.310(a)(2)(i); PISP: 4.11.17	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: PE-17.1

Assessment Objective

Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Assessment Methods And Objects

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

Interview: Organization personnel using alternate work sites.

PE-18 – Location of Information System Components (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that information system components are positioned 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, 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.

Applicability: All	**Reference(s):** ARS: PE-18; FISCAM: AC-6, CP-2; HIPAA: 164.312(c)(1); PISP: 4.11.18	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-18.1

Assessment Objective

Determine if:
(i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards;

(ii) 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

Plan the location or site of information system facilities with regard to physical and environmental hazards and, for existing facilities, consider the physical and environmental hazards in the risk mitigation strategy.

Applicability: All	**Reference(s):** ARS: PE-18(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-18(1).1

Assessment Objective

Determine if:
(i) the organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards;

(ii) 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.

PE-19 – Information Leakage (Optional) (High)

Control

Safeguards and countermeasures should be considered to protect information systems against information leakage due to electromagnetic signals emanations.

Guidance

The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Applicability: Optional for all	**Reference(s):** ARS: PE-19; FISCAM: AC-4; PISP: 4.11.19	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-19.1

Assessment Objective

Determine if the organization protects the information system from information leakage due to electromagnetic signals emanations.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing information leakage due to electromagnetic signals emanations; mechanisms protecting the

information system against electronic signals emanation; facility housing the information system; records from electromagnetic signals emanation tests; other relevant documents or records.

Test: Information system for information leakage due to electromagnetic signals emanations.

Planning (PL) – *Management*

PL-1 – Security Planning Policy and Procedures (High)

Control

All CMS information systems and major applications shall be documented in a SSP, which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, in accordance with current CMS Procedures.

Guidance

The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-18 provides guidance on security planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: PL-1; 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; PISP: 4.12.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents security planning policy and procedures;
(ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review security planning policy and procedures;
(iv) the organization updates security planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with security planning responsibilities.

ASSESSMENT PROCEDURE: PL-1.2

Assessment Objective

Determine if:
(i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;
(iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security planning controls.

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

All CMS information systems and major applications shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18.

The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Implementation Standard(s)

1. (For PHI only) Retain documentation of policies and procedures relating to HIPAA 164.306 for 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 is aligned with the organization's information system architecture and information security architecture. NIST SP 800-18 provides guidance on security planning.

Applicability: All	**Reference(s):** ARS: PL-2; 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; PISP: 4.12.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-2.1

Assessment Objective

Determine if:
(i) the organization develops and implements a System Security Plan for the information system;

(ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements;

(iii) the organization defines in the System Security Plan, explicitly or by reference, the values for all organization-defined parameters (i.e., assignment and selection operations) in applicable security controls and control enhancements;

(iv) the System Security Plan development is consistent with NIST Special Publication 800-18;

(v) the System Security Plan is consistent with the organization's information system architecture and information security architecture;

(vi) designated organizational officials review and approve the System Security Plan.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing System Security Plan development and implementation; NIST Special Publication 800-18; System Security Plan; other relevant documents or records.

PL-3 – System Security Plan Update (High)

Control

The SSP shall be reviewed at least every 365 days and updated minimally every three (3) years to reflect current conditions or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security; when the data sensitivity level increases; after a serious security violation; due to changes in the threat environment; or before the previous accreditation expires.

Guidance

Significant changes are defined in advance by the organization and identified in the configuration management process. NIST SP 800-18 provides guidance on security plan

updates.

Applicability: All	**Reference(s):** ARS: PL-3; FISCAM: AS-1, CM-5, SM-1; HIPAA: 164.306(a)(3), 164.316(a), 164.316(b)(2)(iii); HSPD 7: G(24), J(35); IRS-1075: 5.6.1.2#1.4; PISP: 4.12.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-3.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of System Security Plan reviews/updates and the frequency is at least annually;

(ii) the organization updates the System Security Plan in accordance with organization-defined frequency;

(iii) the organization defines in the update to the System Security Plan, explicitly or by reference, the values for all organization-defined parameters (i.e., assignment and selection operations) in applicable updated security controls and control enhancements;

(iv) the organization receives input to update the System Security Plan from the organization's configuration management and control process;

(v) the updated System Security Plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing System Security Plan updates; System Security Plan; configuration management policy and procedures; configuration management documents; record of System Security Plan reviews and updates; other relevant documents or records.

PL-4 – Rules of Behavior (ROB) (High)

Control

ROBs shall be established in alignment HHS requirements http://hhs.gov/ocio/policy/2008-0001.003s.html, and made readily available, to delineate clearly user responsibilities and expected behavior of all Business Owners, users, operators, and administrators with regard to information and information system usage. Before authorizing access to the information system and / or information and annually thereafter, the organization shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the ROBs. Specific ROBs shall be established to govern work-at-home users who access CMS information or information systems.

Limited personal use of organization-owned or leased equipment and resources shall be considered to be a permitted use of organization-owned or leased equipment and resources when the following conditions are met:
4.12.4.1. Such use involves minimal additional expense to CMS;
4.12.4.2. Such use does not interfere with the mission or operation of CMS;
4.12.4.3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch;
4.12.4.4. Such use does not overburden any CMS information system resources;
4.12.4.5. Such use is not otherwise prohibited under this policy; and
4.12.4.6. Any use of organizational Internet and email resources shall be made with the understanding that such use is not secure, private or anonymous.

The following uses of organization-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited:
4.12.4.7. Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace;
4.12.4.8. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords;
4.12.4.9. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity;
4.12.4.10. All email communications to groups of employees that are subject to approval prior to distribution and have not been approved by the organization (e.g., retirement announcements, union notices or announcements, charitable solicitations); and
4.12.4.11. Employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees.

All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of organization-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that

employees desire to protect their privacy, employees shall not use organization-owned or leased equipment and resources.

Implementation Standard(s)

1. Define user roles and expectations for system and network use.
2. Electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).

Guidance

Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST SP 800-18 provides guidance on preparing rules of behavior.

Applicability: All	**Reference(s):** ARS: PL-4; FISCAM: CP-2, SM-4; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.5; PISP: 4.12.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-4.1

Assessment Objective

Determine if:
(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information and information system usage;

(ii) the organization makes the rules available to all information system users;

(iii) the rules of behavior for organizational personnel are consistent with NIST Special Publication 800-18;

(iv) 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 the information system and its resident information.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing rules of behavior for information system users; NIST Special Publication 800-18; 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

PIAs shall be conducted for CMS information systems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandum M-03-22, and the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations.

Guidance

OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

Applicability: All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC	**Reference(s):** ARS: PL-5; FISCAM: SM-5; HSPD 7: J(35); PISP: 4.12.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-5.1

Assessment Objective

Determine if:
(i) the organization conducts a privacy impact assessment on the information system;

(ii) the privacy impact assessment is compliant with OMB policy.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing privacy impact assessments on the information system; appropriate federal legislation and OMB policy; privacy impact assessment; other relevant documents or records.

PL-6 – Security-Related Activity Planning (High)

Control

Security-related activities affecting the information system shall be planned and coordinated before being performed in order to reduce the impact on CMS operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing / exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Guidance

Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Applicability: All	**Reference(s):** ARS: PL-6; FISCAM: SM-1; PISP: 4.12.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-6.1

Assessment Objective

Determine if:
(i) 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, organizational assets, and individuals;

(ii) the organization's advance planning and coordination of security-related activities includes both emergency and non-emergency situations.

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.

Personnel Security (PS) – *Operational*

PS-1 – Personnel Security Policy and Procedures (High)

Control

CMS information systems shall employ personnel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines. Procedures shall be developed to guide the implementation of personnel security controls.

Guidance

The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	Reference(s): ARS: PS-1; FISCAM: AS-1, SD-2, SM-1, SM-3, SM-4; IRS-1075: 5.6.2.1#1.1-2; PISP: 4.13.1	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: PS-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents personnel security policy and procedures;
(ii) the organization disseminates personnel security policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review personnel security policy and procedures;
(iv) the organization updates personnel security policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Personnel security policy and procedures, other relevant documents or records.

Interview: Organizational personnel with personnel security responsibilities.

ASSESSMENT PROCEDURE: PS-1.2

Assessment Objective

Determine if:
(i) the personnel security policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the personnel security policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;
(iii) the personnel security procedures address all areas identified in the personnel security policy and address achieving policy-compliant implementations of all associated personnel security controls.

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

A criticality / sensitivity rating (e.g., non-sensitive, national security, public trust) shall be assigned to all positions within the organization. The criticality / sensitivity rating shall be in compliance with 5 CFR 731.106(a), Executive Orders 10450 and 12968, NSPD-1, HSPD-7, and HSPD-12 and consistent with OPM policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating. All criticality / sensitivity ratings must be submitted to the DHHS HR department and CMS' personnel security department.

Implementation Standard(s)

1. Review and revise position risk designations every 365 days.

Guidance

Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Applicability: All	**Reference(s):** ARS: PS-2; FISCAM: SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.3; PISP: 4.13.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-2.1

Assessment Objective

Determine if:
(i) the organization assigns a risk designations to all positions within the organization;

(ii) the organization establishes a screening criteria for individuals filling organizational positions;

(iii) the risk designations for the organizational positions are consistent with 5 CFR 731.106(a) and OPM policy and guidance;

(iv) the organization defines in the System Security Plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions;

(v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; System Security Plan; records of risk designation reviews and updates; other relevant documents or records.

PS-3 – Personnel Screening (High)

Control

Prior to being granted access, all employees and contractors who require access to CMS information or information systems shall be screened and reinvestigated periodically, consistent with the criticality / sensitivity rating of the position. For prospective employees, references background checks shall be performed before issuance of a User ID. Security agreements shall be required for employees and contractors assigned to work with mission critical information.

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 is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and SP 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.

Applicability: All	**Reference(s):** ARS: PS-3; FISCAM: AC-6, SM-4, SM-7; IRS-1075: 5.6.2.1#1.4; PISP: 4.13.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-3.1

Assessment Objective

Determine if:
(i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access;

(ii) 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.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; FIPS 201; NIST Special Publications 800-73, 800-78; other relevant documents or records.

PS-4 – Personnel Termination (High)

Control

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information and information systems is removed upon personnel termination. Termination procedures shall address:
4.13.4.1. Exit interviews;
4.13.4.2. Retrieval of all organizational information system-related property;
4.13.4.3. Notification to security management;
4.13.4.4. Revocation of all system access privileges;
4.13.4.5. Immediately escorting employees terminated for cause out of organization facilities; and
4.13.4.6. Hard disk back up and sanitization before re-issuance.

Appropriate personnel shall have access to official records created by the terminated employee that are stored on organizational information systems.

Implementation Standard(s)

1. Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

Guidance

Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Applicability: All	**Reference(s):** ARS: PS-4; FISCAM: SM-4; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: 5.6.2.1#1.5; PISP: 4.13.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-4.1

Assessment Objective

Determine if:
(i) the organization terminates information system access upon termination of individual employment;
(ii) the organization conducts exit interviews of terminated personnel;
(iii) the organization retrieves all organizational information system-related property from terminated personnel;
(iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.

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

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information or information systems no longer required in the new assignment is terminated upon personnel transfer. Transfer procedures shall address:

4.13.5.1. Re-issuing appropriate organizational information system-related property (e.g., keys, identification cards, building passes);

4.13.5.2. Notification to security management;
4.13.5.3. Closing obsolete accounts and establishing new accounts; and
4.13.5.4. Revocation of all system access privileges (if applicable).

Guidance

Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts.

Applicability: All	**Reference(s):** ARS: PS-5; FISCAM: SM-4; IRS-1075: 5.6.2.1#1.6; PISP: 4.13.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-5.1

Assessment Objective

Determine if:
(i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization;

(ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; changing system access authorization) for personnel reassigned or transferred within the organization.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

PS-6 – Access Agreements (High)

Control

Individuals who require access to CMS information or information systems shall be required to complete and sign appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements.

Implementation Standard(s)

1. Access agreements are reviewed and updated as part of the system accreditation 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. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Applicability: All	**Reference(s):** ARS: PS-6; FISCAM: AC-6, AS-1, SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.7; PISP: 4.13.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-6.1

Assessment Objective

Determine if:
(i) the organization requires appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access;

(ii) organizational personnel sign appropriate access agreements prior to receiving access;

(iii) the organization defines in the System Security Plan, explicitly or by reference, the frequency of reviews/updates for access agreements;

(iv) 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; System Security Plan; access agreements; records of access agreement reviews and updates; other relevant documents or records.

PS-7 – Third-Party Personnel Security (High)

Control

Personnel security controls employed by external service providers and third parties shall be documented, agreed to, implemented effectively, and monitored for compliance and shall include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements. Personnel security controls employed by service providers and third parties shall be compliant with CMS IS policies and procedures, and consistent with NIST SP 800-35.

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. NIST SP 800-35 provides guidance on information technology security services.

Applicability: All	Reference(s): ARS: PS-7; FISCAM: AC-6, AS-1, SD-1, SM-4, SM-7; IRS-1075: 5.6.2.1#1.8; PISP: 4.13.7	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: PS-7.1

Assessment Objective

Determine if:
(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management);

(ii) the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35;

(iii) the organization monitors third-party provider compliance with personnel security requirements.

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 shall enforce formal personnel sanctions process for personnel who fail to comply with established CMS IS policies and procedures. The employee sanction process shall be consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines.

Guidance

The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Applicability: All	Reference(s): ARS: PS-8; FISCAM: AC-5, SD-2, SM-4; HIPAA: 164.308(a)(1)(ii)(C); PISP: 4.13.8	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: PS-8.1

Assessment Objective

Determine if:

(i) the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures;

(ii) the personnel sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

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

PS-CMS-1 – Review System Access during Extraordinary Personnel Circumstances (High)

Control

Access to CMS information and information systems shall be reviewed during extraordinary personnel circumstances and limited as deemed necessary.

Guidance

Personnel are an organizational resource and can impact the Confidentiality, Integrity and Availability (CIA) of CMS data. If by the organizations' management's view, CIA is impaired by the individual's actions and the individual is not or can not perform his/her duties to meet the organization's security standards then the individual's access to CMS sensitive information systems should be curtailed or terminated. Organizations should implement Human Relation (HR) policies to manage and handle personnel issues in compliance with this requirement. The organization's policies should allow the individual's manager or supervisor to initiate action(s) when extraordinary circumstance information becomes available.

Applicability: All	**Reference(s):** ARS: PS-9; FISCAM: SD-2; PISP: 4.13.9	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-CMS-1.1

Assessment Objective

Determine if the organization manages personnel with extraordinary personal circumstances.

Assessment Methods And Objects

Examine: Personnel security policy and procedures; other relevant documents or records determine system access during extraordinary personnel circumstances is reviewed and access is limited as deemed necessary.

Interview: Organizational personnel with personnel security responsibilities to determine system access during extraordinary personnel circumstances is reviewed and access is limited as deemed necessary.

PS-CMS-2 – Designate an Information System Security Officer (ISSO) / System Security Officer (SSO) (High)

Control

An Information System Security Officer (ISSO) / System Security Officer (SSO) shall be designated for each business component with roles and responsibilities of the position clearly defined.

Guidance

A good reference set for defining the Information System Security Officer (ISSO) / System Security Officer (SSO) responsibilities are the NIST SPs. Specific responsibilities should be developed to protect CMS information systems and data.

Applicability: All	**Reference(s):** ARS: PS-10; FISCAM: SM-1; HIPAA: 164.308(a)(2); PISP: 4.13.10	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-CMS-2.1

Assessment Objective

Determine if the organization has documented the roles and responsibilities of appointed ISSO / SSO.

Assessment Methods And Objects

Examine: Personnel security policy and procedures; other relevant documents or records to determine an ISSO / SSO is designated for each component with roles and responsibilities of the position clearly defined.

Interview: Organizational personnel with personnel security responsibilities to determine an ISSO / SSO is designated for each component with roles and responsibilities of the

position clearly defined.

Risk Assessment (RA) – *Management*

RA-1 – Risk Assessment Policy and Procedures (High)

Control

All CMS applications and systems shall be covered by an IS RA. The RA shall be consistent with NIST SP 800-30. Formal documented procedures shall be developed, disseminated, and reviewed / updated periodically to facilitate the implementation of the RA policy and associated RA controls. The procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-30 provides guidance on the assessment of risk. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: RA-1; 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; PISP: 4.14.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: RA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents risk assessment policy and procedures;
(ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization;
(iii) responsible parties within the organization periodically review risk assessment policy and procedures;
(iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

ASSESSMENT PROCEDURE: RA-1.2

Assessment Objective

Determine if:
(i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;
(ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;
(iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated risk assessment controls.

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

CMS information systems and the information processed, stored, or transmitted by the systems shall be categorized in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to the, CMS System Security Level by Information Type. The security categorization (including

supporting rationale) shall be explicitly documented. Designated senior-level officials within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the CMS CIO, CISO, and Business Owners.

All CMS information systems categorized as high or moderate shall be considered sensitive or to contain sensitive information. All CMS information systems categorized as low shall be considered non-sensitive or to contain non-sensitive information. All CMS information systems shall implement minimum security requirements and controls as established in the current CMS IS Standards, based on security categorization of the system.

Guidance

The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST SP 800-60 provides guidance on determining the security categories of the information types resident on the information system.

Applicability: All	**Reference(s):** ARS: RA-2; FISCAM: CP-1, SM-2; HSPD 7: D(8); IRS-1075: 4.1#2; PISP: 4.14.2	**Related Controls Requirement(s):** MP-4, SC-7

ASSESSMENT PROCEDURE: RA-2.1

Assessment Objective

Determine if:
(i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners;

(ii) the security categorization is consistent with FIPS 199 and considers the provisional impact levels and special factors in NIST Special Publication 800-60;

(iii) the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts;

(iv) the organization includes supporting rationale for impact-level decisions as part of the security categorization;

(v) designated, senior-level organizational officials review and approve the security categorizations.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST Special Publication 800-60; System Security Plan; other relevant documents or records.

Interview: Organizational personnel with security categorization and risk assessment responsibilities.

RA-3 – Risk Assessment (High)

Control

An assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that support the operations and assets of CMS shall be performed, both within CMS and by external parties that manage / operate information or information systems for CMS. The RA shall be in accordance with current CMS Procedures. Based on the operation of the information system, the RA shall take into account vulnerabilities, threat sources, and security controls in place to determine the resulting level of residual risk posed to CMS operations, CMS assets, CMS information, or individuals.

Any findings from reviews of CMS systems shall be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses shall be documented by the Business Owner or external party and addressed by mitigating the risk, accepting the risk with explanation or submitting Corrective Action Plan (CAP). These findings shall be subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Implementation Standard(s)

1. Perform an IS RA for the system, and document the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]).

Guidance

Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST SP 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Applicability: All	**Reference(s):** ARS: RA-3; 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; PISP: 4.14.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: RA-3.1

Assessment Objective

Determine if:
(i) the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties);

(ii) the IS RA is consistent with the NIST Special Publication 800-30.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; IS RA; NIST Special Publication 800-30; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

RA-4 – Risk Assessment Update (High)

Control

The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation.

Guidance

The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates.

Applicability: All	**Reference(s):** ARS: RA-4; FISCAM: AS-1, CM-5, SD-2, SM-2; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 5.6.1.1#1.4; PISP: 4.14.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: RA-4.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of IS RA updates;

(ii) the organization develops and documents specific criteria for what is considered significant change to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system;

(iii) the organization updates the IS RA in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system;

(iv) the IS RA update is consistent with the NIST Special Publications 800-30.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing IS RA updates; IS RA; System Security Plan; records of risk assessment updates; NIST Special Publication 800-30; other relevant documents or records.

RA-5 – Vulnerability Scanning (High)

Control

Appropriate vulnerability assessment tools and techniques shall be implemented by the organization. Selected personnel shall be trained in their use and maintenance. The organization shall conduct periodic testing of its security posture by scanning its information systems with vulnerability tools. The information obtained from the vulnerability scanning process shall be shared with appropriate personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems. The activities of employees using organization Internet and email resources shall be subject to monitoring by system or security personnel without notice.

Implementation Standard(s)

1. Utilize appropriate vulnerability scanning tools and techniques to scan for vulnerabilities in the information system every 90 days or when significant new vulnerabilities are identified and reported.
2. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once every 365 days, in accordance with CMS IS procedures. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.

Guidance

Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST SP 800-42 provides guidance on network security testing. NIST SP 800-40 (Version 2) provides guidance on patch and vulnerability management.

Applicability: All	**Reference(s):** ARS: RA-5; FISCAM: CM-5, SM-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); PISP: 4.14.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: RA-5.1

Assessment Objective

Determine if:

(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of vulnerability scans within the information system;

(ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency and/or random in accordance with organizational policy and assessment of risk, or when significant new vulnerabilities potentially affecting the system are identified and reported;

(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans;

(iv) the organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques;

(v) the organization freely shares the information obtained from the vulnerability scanning process with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; IS RA; System 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

Vulnerability scanning tools must include the capability to readily update the list of vulnerabilities scanned.

Applicability: All	**Reference(s):** ARS: RA-5(1); 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; risk assessment; vulnerability scanning tools and techniques documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.

Test: Vulnerability scanning capability and associated scanning tools.

RA-5(2) – Enhancement (High)

Control

Update the list of system vulnerabilities scanned every 365 days or when significant new vulnerabilities are identified and reported.

Applicability: All	**Reference(s):** ARS: RA-5(2); 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:
(i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of updates for information system vulnerabilities scanned;

(ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when significant new vulnerabilities are identified and reported.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; IS RA; System Security Plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records.

RA-5(3) – Enhancement (High)

Control

Perform internal network penetration testing as needed but no less than once a year, in accordance with the CMS IS procedures. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention.

Applicability: All	**Reference(s):** ARS: RA-5(3); 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:
(i) the organization implements procedures that can demonstrate the breadth of scan coverage (including information system components scanned);

(ii) the organization implements procedures that can demonstrate the depth of scan coverage (including vulnerabilities checked.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; IS RA; list of vulnerabilities scanned and information system components checked; other

relevant documents or records.

System and Services Acquisition (SA) – *Management*

SA-1 – System and Services Acquisition Policy and Procedures (High)

Control

Documented procedures shall be developed and implemented effectively to facilitate the implementation of the system and services acquisition security controls in all system and services acquisitions. Procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Implementation Standard(s)

1. (For FTI only) Develop, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes IRS documents received and identified by:
(a) taxpayer name
(b) tax year(s)
(c) type of information (e.g., revenue agent reports, Form 1040, work papers)
(d) the reason for the request
(e) date requested
(f) date received
(g) exact location of the FTI
(h) who has had access to the data and
(i) if disposed of, the date and method of disposition.

Guidance

The system and services acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: SA-1; FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.1.3#1.1-2; PISP: 4.15.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and services acquisition policy and procedures;

(ii) the organization disseminates system and services acquisition policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and services acquisition policy and procedures;

(iv) the organization updates system and services acquisition policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities.

ASSESSMENT PROCEDURE: SA-1.2

Assessment Objective

Determine if:
(i) the system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and services acquisition policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and

guidance;

(iii) the system and services acquisition procedures address all areas identified in the system and services acquisition policy and address achieving policy-compliant implementations of all associated system and services acquisition controls.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities.

SA-2 – Allocation of Resources (High)

Control

As part of the capital planning and investment control processes, CMS or the external organization shall determine, document, and allocate the resources required to protect CMS information systems adequately. IS requirements shall be included in mission / business case planning, and a separate line item shall be established in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Guidance

The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST SP 800-65 provides guidance on integrating security into the capital planning and investment control process.

Applicability: All	**Reference(s):** ARS: SA-2; FISCAM: CM-3, IN-2, SD-1, SM-1; PISP: 4.15.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-2.1

Assessment Objective

Determine if the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system by verifying that the organization:
- defines security requirements for the information system in mission/business planning;
- establishes a discrete line item for information system security in the organization's programming and budgeting documentation;
- integrates information system security into the capital planning and investment control process in accordance with the guidance in NIST Special Publication 800-65.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST Special Publication 800-65; other relevant documents or records.

Interview: Organizational personnel with capital planning and investment responsibilities.

SA-3 – Life Cycle Support (High)

Control

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

Implementation Standard(s)

1. Must comply with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

Guidance

NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Applicability: All	**Reference(s):** ARS: SA-3; 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; PISP: 4.15.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-3.1

Assessment Objective

Determine if:
(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations;

(ii) the organization uses a system development life cycle that is consistent with NIST Special Publication 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST Special Publication 800-64; 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

Security requirements and/or security specifications shall be included, either explicitly or by reference, in all information system acquisition contracts based on an assessment of risk in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

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:
4.15.4.1. Security capabilities;
4.15.4.2. Design and development processes;
4.15.4.3. Test and evaluation procedures; and
4.15.4.4. Documentation.

The requirements in the solicitation documents shall permit updating security controls as new threats / vulnerabilities are identified and as new technologies are implemented

Use of Evaluated and Validated Products
For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet 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.

Configuration Settings and Implementation Guidance
The information system required documentation shall include security configuration settings, including documentation explaining exceptions to the standard, and security implementation guidance.

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

Solicitation Documents
The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (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. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST SP 800-36 provides guidance on the selection of information security products. NIST SP

800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Information System Documentation
The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

Use of Tested, Evaluated, and Validated Products
NIST SP 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.

Configuration Settings and Implementation Guidance
The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on configuration settings for information technology products.

Applicability: All	**Reference(s):** ARS: SA-4; FISCAM: AS-1, CM-3, SM-7; PISP: 4.15.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-4.1

Assessment Objective

Determine if:
(i) the organization includes in acquisition contracts for information systems, either explicitly or by reference, security requirements and/or security specifications based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards that describe required:
- security capabilities;
- design and development processes;
- test and evaluation procedures;
- documentation.

(ii) the organization includes in acquisition contracts, requirements for information system documentation addressing user and systems administrator guidance and information regarding the implementation of the security controls in the system and at a level of detail based on the FIPS 199 security category for the system.;

(iii) the organization includes in acquisition contracts requirements for information system documentation that includes security configuration settings and security implementation guidance.

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; NIST Special Publications 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.

SA-4(1) – Enhancement (High)

Control

Ensure solicitation documents require that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Applicability: All	**Reference(s):** ARS: SA-4(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-4(1).1

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with 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-5 – Information System Documentation (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

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. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.
4. Document the system's configuration, and procedures in support of system access administration and operations.

Guidance

Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Applicability: All	**Reference(s):** ARS: SA-5; 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; PISP: 4.15.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-5.1

Assessment Objective

Determine if:
(i) the organization obtains, protects as required, and makes available to authorized personnel, information system administrator and user guidance with information on:
- configuring, installing, and operating the information system;
- effectively using the system's security features; or

(ii) the organization, when this information is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; 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:
(i) 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.

(ii) the organization disseminates information system documentation to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review information system documentation;

(iv) 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

Ensure that system documentation describes the functional properties of the security controls implemented within the information system with sufficient detail to facilitate analysis and testing of the controls.

Applicability: All	**Reference(s):** ARS: SA-5(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-5(1).1

Assessment Objective

Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

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

Ensure that system documentation describes the design and implementation details of the security controls implemented within the information system with sufficient detail to permit analysis and testing of the controls.

Applicability: All	**Reference(s):** ARS: SA-5(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-5(2).1

Assessment Objective

Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components.

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-6 – Software Usage Restrictions (High)

Control

All software or shareware and associated documentation used on CMS information systems shall be deployed and maintained in accordance with appropriate license agreements and copyright laws. Software associated documentation protected by quantity licenses shall be managed through a tracking system to control copying and distribution. All other uses not specifically authorized by the license agreement shall be prohibited. The use of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Guidance

Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible 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.

Applicability: All	**Reference(s):** ARS: SA-6; FISCAM: CM-3, CM-5; IRS-1075: 4.7.3#1.2; PISP: 4.15.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-6.1

Assessment Objective

Determine if:
(i) the organization complies with software usage restrictions;

(ii) the organization employs tracking systems to control copying and distribution of software and associated documentation protected by quantity licenses;

(iii) the organization controls and documents the use of publicly accessible 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.

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

All users shall be restricted from downloading or installing software, unless explicitly authorized in writing by the CIO or his/her designated representative. Users that have been granted such authorization may download and install only organization-approved software. The use of install-on-demand software shall be restricted.

Implementation Standard(s)

1. If user installed software is authorized in writing by the CIO or his/her designated representative, 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 that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Applicability: All	**Reference(s):** ARS: SA-7; FISCAM: CM-3, CM-5; PISP: 4.15.7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-7.1

Assessment Objective

Determine if the organization enforces explicit rules governing the installation of software by users that include organization-identified types of software installations that are permitted and types of installations that are prohibited.

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.

Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.

Test: Enforcement of rules for user installed software on the information system; information system for prohibited software.

SA-8 – Security Engineering Principles (High)

Control

CMS information systems shall be designed and implemented using accepted security engineering principles.

Implementation Standard(s)

1. Design and implement the information system using the security engineering principles detailed in NIST SP 800-27 Rev. A, Engineering Principles for IT Security (A Baseline for Achieving Security).

Guidance

NIST SP 800-27 provides guidance on engineering principles for information system security. 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 components within the system.

Applicability: All	**Reference(s):** ARS: SA-8; FISCAM: BP-2, BP-4, CM-3; PISP: 4.15.8	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-8.1

Assessment Objective

Determine if:
(i) the organization designs and implements the information system using security engineering principles;

(ii) the organization considers the security design principles in NIST Special Publication 800-27 in the design, development, and implementation 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; NIST Special Publication 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities.

SA-9 – External Information System Services (High)

Control

All external information system services shall include specific provisions requiring the service provider to comply with CMS IS policies, standards, and guidelines; and shall be monitored for compliance. CMS shall define the remedies for any loss, disruption, or damage caused by the service provider's failure to comply. Service providers shall be prohibited from outsourcing any system function overseas, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representatives with concurrence from CMS' personnel security department.

Implementation Standard(s)

1. If service providers are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas, ensure that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.
2. (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 accreditation 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., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system 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 service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. 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 to its operations and assets, or to individuals. 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 non-compliance. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on the security considerations in the system development life cycle.

Applicability: All	**Reference(s):** ARS: SA-9; FISCAM: AS-1, SM-7; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4; PISP: 4.15.9	**Related Controls Requirement(s):** CA-3

ASSESSMENT PROCEDURE: SA-9.1

Assessment Objective

Determine if:
(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;

(ii) the organization monitors security control compliance.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

SA-10 – Developer Configuration Management (High)

Control

Information system developers shall develop, document, and implement a configuration management plan for each information system under development. The configuration management plan shall address change control mechanisms during development, change authorization requirements, and security flaw identification, tracking, and remediation processes.

Guidance

This control also applies to the development actions associated with information system changes.

Applicability: All	**Reference(s):** ARS: SA-10; FISCAM: AS-1, AS-3, BP-2, BP-4, CM-3, CM-4, CM-6, CP-2, DA-1; PISP: 4.15.10	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-10.1

Assessment Objective

Determine if the organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

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.

SA-11 – Developer Security Testing (High)

Control

Information system developers shall develop, document, and implement a security test and evaluation (ST&E) plan for each information system under development in accordance with, but not limited to the, current CMS Procedures. The developer security test results shall be documented.

Implementation Standard(s)

1. If the Security Test and Evaluation (ST&E) results are used in support of the security C&A process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the security testing and after selective verification of the results.
2. Use hypothetical data when executing test scripts.

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 certification and accreditation 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 (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.

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; other relevant documents or records.

System and Communications Protection (SC) – *Technical*

SC-1 – System and Communications Protection Policy and Procedures (High)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	**Reference(s):** ARS: SC-1; FISCAM: AS-1, CM-5, SM-1, SM-3; IRS-1075: 5.6.3.4#1, 5.6.3.4#2; PISP: 4.16.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and communications protection policy and procedures;

(ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and communications protection policy and procedures;

(iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required.

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.

ASSESSMENT PROCEDURE: SC-1.2

Assessment Objective

Determine if:
(i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated system and communications protection controls.

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

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Implementation Standard(s)

1. Place all CMS servers allowing public access within a DMZ environment, and disallow direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Guidance

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Applicability: All	**Reference(s):** ARS: SC-2; FISCAM: AC-4, AS-2, DA-1; PISP: 4.16.2	**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

Information system security functions shall be isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system shall maintain a separate execution domain (e.g., address space) for each executing process.

Guidance

The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and 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):** ARS: SC-3; FISCAM: AC-4; PISP: 4.16.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-3.1

Assessment Objective

Determine if:
(i) the organization defines the security functions of the information system to be isolated from nonsecurity functions;

(ii) the information system isolates security functions from nonsecurity functions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Separation of security functions from nonsecurity functions within the information system.

SC-3(1) – Enhancement (High)		
Control Employ hardware separation mechanisms to facilitate the isolation of security functions.		
Applicability: All	**Reference(s):** ARS: SC-3(1)	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SC-3(1).1		
Assessment Objective Determine if the information system employs 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 Isolate critical security functions from both non-security functions and other security functions.		
Applicability: All	**Reference(s):** ARS: SC-3(2)	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SC-3(2).1		
Assessment Objective Determine if the information system isolates security functions enforcing access and information flow control from both nonsecurity functions and from other security functions. **Assessment Methods And Objects** **Examine:** System and communications protection policy; procedures addressing security function isolation; list of critical security functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. **Test:** Isolation of critical security functions.		
SC-3(3) – Enhancement (High)		
Control Minimize the number of non-security functions included within the isolation boundary containing security functions.		
Applicability: All	**Reference(s):** ARS: SC-3(3)	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SC-3(3).1		
Assessment Objective Determine if the information system minimizes the number of nonsecurity functions included within the isolation 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 Implement security functions in largely independent modules that avoid unnecessary interactions between modules.		

Applicability: All	Reference(s): ARS: SC-3(4)	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: SC-3(4).1

Assessment Objective

Determine if the information system security functions are implemented 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

Implement security functions in 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): ARS: SC-3(5)	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: SC-3(5).1

Assessment Objective

Determine if the information system security functions are implemented 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 Remnance (High)

Control

No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.

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 PII 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 PII 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

Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of 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.

Applicability: All	Reference(s): ARS: SC-4; FISCAM: AC-4; IRS-1075: 5.6.3.4#2, 5.6.3.4#3; PISP: 4.16.4	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.

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.

Test: Information system for unauthorized and unintended transfer of information via shared system resources.

SC-5 – Denial of Service Protection (High)

Control

Mechanisms shall be established to prevent, or limit the effects of well-known, detectable, and preventable denial-of-service attacks.

Implementation Standard(s)

1. Protect the information system against the denial-of-service attacks defined on the following sites or within 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. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Applicability: All	**Reference(s):** ARS: SC-5; FISCAM: AC-5; PISP: 4.16.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-5.1

Assessment Objective

Determine if:
(i) the organization defines in the System 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;

(ii) 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; System 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-5(1) – Enhancement (High)

Control

Restrict the ability of users to launch denial of service attacks against other information systems or networks.

Applicability: All	**Reference(s):** ARS: SC-5(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-5(1).1

Assessment Objective

Determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; 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-5(2) – Enhancement (High)

Control

Maintain excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

Applicability: All	**Reference(s):** ARS: SC-5(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-5(2).1

Assessment Objective

Determine if the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding 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; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing information system bandwidth, capacity, and redundancy management.

SC-6 – Resource Priority (High)

Control

Mechanisms shall be implemented to provide for allocation of information system resources based upon priority. Priority protection shall ensure that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.

Applicability: All	**Reference(s):** ARS: SC-6; FISCAM: AC-3; PISP: 4.16.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-6.1

Assessment Objective

Determine if the information system limits the use of resources by priority.

Assessment Methods And Objects

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

Test: Automated mechanisms implementing resource allocation capability.

SC-7 – Boundary Protection (High)

Control

Automated boundary protection mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces. The operational failure of the boundary protection mechanisms shall not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing site shall provide the same levels of protection as those of the primary site.

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

Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.
The organization carefully 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. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-77 provides guidance on virtual private networks.

Applicability: All	**Reference(s):** ARS: SC-7; FISCAM: AC-1, AS-2; PISP: 4.16.7	**Related Controls Requirement(s):** AC-4, CA-3, MP-4, RA-2

ASSESSMENT PROCEDURE: SC-7.1

Assessment Objective

Determine if:
(i) the organization defines key internal boundaries of the information system;
(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

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; 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

Physically allocate publicly-accessible information system components (e.g., public web servers, public email servers, public DNS servers) to separate sub-networks with separate physical network interfaces.

Guidance

Publicly accessible information system components include, for example, public web servers.

Applicability: All	**Reference(s):** ARS: SC-7(1)	**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

Prevent public access into the internal networks except as appropriately mediated.

Applicability: All	**Reference(s):** ARS: SC-7(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-7(2).1

Assessment Objective

Determine if:
(i) the organization defines the mediation necessary for public access to the organization's internal networks;

(ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.

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

Limit the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

Applicability: All	**Reference(s):** ARS: SC-7(3)	**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 better monitoring of inbound and outbound 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; other relevant documents or records.

SC-7(4) – Enhancement (High)

Control

Maintain a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

Applicability: All	**Reference(s):** ARS: SC-7(4)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-7(4).1

Assessment Objective

Determine if the organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service,

implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.

SC-7(5) – Enhancement (High)

Control

Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.

Applicability: All	**Reference(s):** ARS: SC-7(5)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-7(5).1

Assessment Objective

Determine if the information system denies network traffic by default and 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-8 – Transmission Integrity (High)

Control

Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the integrity of CMS information while in transit.

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, Use of Cryptography, PISP 4.16.13).

Guidance

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 either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission integrity using IPSec. NIST SP 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Applicability: All	**Reference(s):** ARS: SC-8; FISCAM: AC-4; HIPAA: 164.312(c)(1); PISP: 4.16.8	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-8.1

Assessment Objective

Determine if the information system protects the integrity of transmitted information.

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

Employ approved cryptographic mechanisms to ensure recognition of changes to information during transmission.

Guidance

Alternative physical protection measures include, for example, protected distribution systems.

Applicability: All	**Reference(s):** ARS: SC-8(1); HIPAA: 164.312(c)(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-8(1).1

Assessment Objective

Determine if the information system 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

Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the confidentiality of CMS sensitive information while in transit.

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

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 either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission confidentiality using IPSec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Applicability: All	**Reference(s):** ARS: SC-9; 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; PISP: 4.16.9	**Related Controls Requirement(s):** AC-17

ASSESSMENT PROCEDURE: SC-9.1

Assessment Objective

Determine if the information system protects the confidentiality of transmitted information.

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.

Test: Transmission confidentiality capability within the information system.

SC-9(1) – Enhancement (High)

Control

Encryption is not required within a secured network. When transmitting data outside of a secured network:
(a) An approved encryption method must be used (see SC-13, Use of Cryptography, PISP 4.16.13) (see SC-CMS-4 for E-Mail), and
(b) Either a VPN or dedicated leased lines/circuits must be used.

Guidance

Alternative physical protection measures include, for example, protected distribution systems.

Applicability: All	**Reference(s):** ARS: SC-9(1); 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 information system employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measure.

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

Technical controls shall be established and implemented effectively to ensure that network connections are properly terminated at the end of user sessions, or upon the occurrence of specified conditions (e.g., a period of inactivity).

Implementation Standard(s)

1. Configure the information system to forcibly disconnect network connections at the end of a session, or after thirty (30) minutes of inactivity, for mainframe sessions.

Guidance

The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Applicability: All	**Reference(s):** ARS: SC-10; FISCAM: AC-1, AS-2; PISP: 4.16.10	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-10.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the time period of inactivity before the information system terminates a network connection;
(ii) the information system terminates a network connection at the end of a session or after the organization-defined time period 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.

Test: Network disconnect capability within the information system.

SC-11 – Trusted Path (High)

Control

Technical controls shall be established and implemented effectively to provide the capability to establish trusted communications paths between authorized users and the security functionality of the information system.

Implementation Standard(s)

1. At a minimum, a trusted communications path is established between the user and the following system security functions: system authentication, re-authentication, and key management.

Guidance

A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Applicability: All	**Reference(s):** ARS: SC-11; FISCAM: AC-4; PISP: 4.16.11	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-11.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the security functions within the information system that are included in a trusted communications path;

(ii) the organization-defined security functions include information system authentication and reauthentication;

(iii) the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing trusted communications paths; System Security Plan; information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records.

Test: Automated mechanisms implementing trusted communications paths within the information system.

SC-12 – Cryptographic Key Establishment and Management (High)

Control

When cryptography is required and used within the information system, documented procedures shall be implemented effectively for cryptographic key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect sensitive information shall be controlled and distributed using the NIST SP 800-56 and NIST SP 800-57 approved key management guidance.

Implementation Standard(s)

1. Employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall prohibit the use of encryption keys that are not recoverable by authorized personnel, require senior management approval to authorize recovery of keys by other than the key owner, and comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Guidance

NIST SP 800-56 provides guidance on cryptographic key establishment. NIST SP 800-57 provides guidance on cryptographic key management.

Applicability: All	**Reference(s):** ARS: SC-12; FISCAM: AC-4; IRS-1075: 5.7.1#1; PISP: 4.16.12	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-12.1

Assessment Objective

Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with responsibilities for cryptographic key establishment or management.

Test: Automated mechanisms implementing cryptographic key management and establishment within the information system.

SC-13 – Use of Cryptography (High)

Control

When cryptographic mechanisms are used, procedures shall be developed, documented, and implemented effectively to ensure they comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. All such mechanisms shall be FIPS 140-2 (as amended and revised) compliant and NIST validated.

Guidance

The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates FIPS 140-2 issued by the NIST Cryptographic Module Validation Program and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	**Reference(s):** ARS: SC-13; 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; PISP: 4.16.13	**Related Controls Requirement(s):** AC-17.Std.1, AC-19.Std.1, AC-3, AC-3.Std.1, SC-12.Std.1, SC-8.Std.1, SC-9(1)

ASSESSMENT PROCEDURE: SC-13.1

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms 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; FIPS 140-2 (as amended); NIST Special Publications 800-56 and 800-57; 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

Technical controls shall be developed, documented, and implemented effectively to protect the integrity of the publicly accessible CMS information and applications.

Implementation Standard(s)

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.
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

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):** ARS: SC-14; FISCAM: AC-2, AC-3; PISP: 4.16.14	**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.

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 (High)

Control

Running collaborative computing mechanisms on CMS information systems shall require authorization by the CIO or his/her designated representative. The authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used. Collaborative computing mechanisms shall not be activated remotely.

Implementation Standard(s)

1. If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:
Ensure the information system provides:
(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and
(b) Explicit indication to the local user of the fact that it is in use.

Guidance

Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

Applicability: All	**Reference(s):** ARS: SC-15; FISCAM: AC-3; PISP: 4.16.15	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-15.1

Assessment Objective

Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

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 mechanisms are authorized in writing by the CIO or his/her designated representative:
Provide physical disconnect of cameras or microphones in a manner that supports ease of use.

Applicability: All	**Reference(s):** ARS: SC-15(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-15(1).1

Assessment Objective

Determine if the information system provides physical disconnect of camera and microphone 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-16 – Transmission of Security Parameters (High)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure that CMS information systems reliably associate security parameters with information exchanged between information systems.

Guidance

Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Applicability: All	**Reference(s):** ARS: SC-16; FISCAM: AC-4; PISP: 4.16.16	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-16.1

Assessment Objective

Determine if the information system reliably associates security parameters with information exchanged between information systems.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission of security parameters; 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 supporting reliable transmission of security parameters between information systems.

SC-17 – Public Key Infrastructure Certificates (High)

Control

All public key certificates used within the CMS information system shall be issued in accordance with a defined certification policy and certification practice statement. Registration to receive a public key certificate shall include authorization by a supervisor or a responsible official, and shall be done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

Guidance

For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24. NIST SP 800-32 provides guidance on public key technology. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	**Reference(s):** ARS: SC-17; FISCAM: AC-2, AS-2; PISP: 4.16.17	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-17.1

Assessment Objective

Determine if 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.

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; NIST Special Publication 800-32; other relevant documents or records.

Interview: Organizational personnel with public key infrastructure certificate issuing responsibilities.

SC-18 – Mobile Code (High)

Control

CMS shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause harm to CMS information systems. The organization shall document, monitor, and implement controls for the use of mobile code within the CMS information system. Appropriate officials shall authorize or deny the use of mobile code. The organization shall implement controls and procedures for mobile code in accordance with NIST SP 800-28.

Guidance

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 organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST SP 800-28 provides guidance on active content and mobile code.

Applicability: All	**Reference(s):** ARS: SC-18; FISCAM: AC-4; PISP: 4.16.18	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-18.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously;

(ii) 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 guidance; NIST Special Publication 800-28; 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

CMS shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to harm CMS information systems. The organization shall document, monitor, and implement controls for the use of VoIP within a CMS information system. When VoIP is implemented, the organization shall adhere to the NIST SP 800-58 guidance.

Implementation Standard(s)

1. The use of VoIP must be authorized in writing by the CMS CIO, or his/her designated representative.

Guidance

NIST SP 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.

Applicability: All	**Reference(s):** ARS: SC-19; FISCAM: CM-5; PISP: 4.16.19	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-19.1

Assessment Objective

Determine if:
(i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously;

(ii) 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; NIST Special Publication 800-58; 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

Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

Guidance

This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/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; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment.

Applicability: All	**Reference(s):** ARS: SC-20; FISCAM: AC-2; PISP: 4.16.20	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-20.1

Assessment Objective

Determine if the information system, (if the system provides a name/address resolution service), provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); NIST Special Publication 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing secure name/address resolution service (authoritative source).

SC-20(1) – Enhancement (High)

Control

When the information system is operating as part of a distributed, hierarchical namespace, ensure that it 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 resource records.

Applicability: All	**Reference(s):** ARS: SC-20(1)	**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 and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

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

Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

Guidance

A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST SP 800-81 provides guidance on secure domain name system deployment.

Applicability: All	**Reference(s):** ARS: SC-21; FISCAM: AC-2; PISP: 4.16.21	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-21.1

Assessment Objective

Determine if the information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it 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

Information systems that collectively provide name / address resolution service for an organization shall be fault tolerant and implement 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). If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified. NIST SP 800-81 provides guidance on secure DNS deployment.

Applicability: All	**Reference(s):** ARS: SC-22; FISCAM: AC-2; PISP: 4.16.22	**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 and implement 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; NIST Special Publication 800-81; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms supporting name/address resolution service for fault tolerance and role separation.

SC-23 – Session Authenticity (High)

Control

Technical controls shall be developed, documented, and effectively implemented to ensure that CMS information systems provide 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 implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST SP 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST SP 800-77 provides guidance on the deployment of IPSec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST SP 800-95 provides guidance on secure web services.

Applicability: All	**Reference(s):** ARS: SC-23; FISCAM: AC-2; PISP: 4.16.23	**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; NIST Special Publications 800-52, 800-77, and 800-95; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing session authenticity.

SC-CMS-1 – Desktop Modems (High)

Control

Users are prohibited from installing desktop modems.

Guidance

Desktop Modems allow backdoors into the network putting the CMS data and network at very high risk.

Applicability: All	**Reference(s):** ARS: SC-CMS-1; PISP: 4.16.24	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-CMS-1.1

Assessment Objective

Determine if the organization has implemented a policy which assists in prohibiting the installation of unauthorized desktop modems.

Assessment Methods And Objects

Examine: Organizational policy does not allow unauthorized desktop modems.

SC-CMS-2 – Identify and Detect Unauthorized Modems (High)

Control

Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized modems.

Implementation Standard(s)

1. Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly.

Guidance

It is good practice that management approve any automated tool or utility for checking for unauthorized modems.

Applicability: All	Reference(s): ARS: SC-CMS-2; PISP: 4.16.25	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: SC-CMS-2.1

Assessment Objective

Determine if the organization has an approved automated system to test for unauthorized modems.

Assessment Methods And Objects

Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly.

SC-CMS-3 – Secondary Authentication and Encryption (High)

Control

Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network.

Implementation Standard(s)

1. Enable and force use of application security mechanisms, such as Transport Layer Security (TLS). Utilize CMS-approved encryption and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, biometric).
2. If e-authentication is required and implemented, refer to ARS Appendix D: E-authentication Standard.

Guidance

A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP.

Applicability: All	Reference(s): ARS: SC-CMS-3; FISCAM: AC-4; PISP: 4.16.26	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: SC-CMS-3.1

Assessment Objective

Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit.

Assessment Methods And Objects

Examine: In-transit technical controls implement and documents for sensitive information outside the secure network.

SC-CMS-4 – Electronic Mail (High)

Control

Controls shall be developed, documented, and implemented effectively 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 technical controls for handling sensitive information via e-mail is the NIST SP.

Applicability: All	Reference(s): ARS: SC-CMS-4; FISCAM: AC-4; PISP: 4.16.27	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: SC-CMS-4.1		
Assessment Objective Determine if the organization effectively develops, documents, and implements protections for CMS sensitive information that is sent via e-mail. **Assessment Methods And Objects** **Examine:** Documentation to determine if all e-mail messages with CMS sensitive information are transmitted using protective measures. **Interview:** Organizational personnel to determine if all e-mail messages with CMS sensitive information is protected, controlled, and monitored.		
SC-CMS-5 – Persistent Cookies (High)		
Control The use of persistent cookies on a CMS web site is prohibited unless explicitly approved in writing by the DHHS Secretary.		
Guidance Requests to DHHS should be via CMS.		
Applicability: All	**Reference(s):** ARS: SC-CMS-5; PISP: 4.16.28	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SC-CMS-5.1		
Assessment Objective Determine if the organization does not use a persistent cookie configuration on a CMS web site to remember subsequent visits unless approved in writing by the DHHS Secretary. **Assessment Methods And Objects** **Examine:** CMS web site baseline and change management documentation for configurations using persistent cookies. **Interview:** Web site administrators to determine if the CMS web site has persistent cookies enable in the baseline configuration or have written approval to enable persistent cookies from the DHHS Secretary.		
SC-CMS-6 – Network Interconnection (High)		
Control Controls shall be developed, documented, and implemented effectively to ensure that only properly authorized network interconnections external to the system boundaries are established. **Implementation Standard(s)** 1. Ensure remote location(s) (e.g., users and sites using a network interconnection external to the system boundaries) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location.		
Guidance A good place to obtain technical controls for securing interconnections external to the system boundaries is the NIST SP.		
Applicability: All	**Reference(s):** ARS: SC-CMS-6; FISCAM: AC-1; PISP: 4.16.29	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SC-CMS-6.1		
Assessment Objective Determine if the organization effectively documents and implements authorized network interconnections external to the system boundaries. **Assessment Methods And Objects** **Examine:** Documentation to determine remote location(s) follow all CMS IS policies and standards for all external interconnections.		

System and Information Integrity (SI) – *Operational*

SI-1 – System and Information Integrity Policy and Procedures (High)

Control

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems, software, and information. The procedures and automated mechanisms shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. 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. NIST SP 800-12 provides guidance on security policies and procedures. It is good practice to have an automated system which is host based to automatically detect, block/filter and alert supervisors or managers that possible unauthorized changes to software and the information system have occurred.

Applicability: All	**Reference(s):** ARS: SI-1; 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; PISP: 4.17.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-1.1

Assessment Objective

Determine if:
(i) the organization develops and documents system and information integrity policy and procedures;

(ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and information integrity policy and procedures;

(iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.

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.

ASSESSMENT PROCEDURE: SI-1.2

Assessment Objective

Determine if:
(i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance;

(iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated system and information integrity controls.

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

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. The flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

Implementation Standard(s)

1. Correct identified information system flaws on production equipment within seventy-two (72) hours.
(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 information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. It is a good practice to test the changes in a laboratory environment on like systems prior to approving and implementing the updates and changes. NIST SP 800-40, provides guidance on security patch installation and patch management.

Applicability: All	**Reference(s):** ARS: SI-2; FISCAM: AS-3, CM-5; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; PISP: 4.17.2	**Related Controls Requirement(s):** CA-2, CA-4, CA-7, CM-3, IR-4, SI-11

ASSESSMENT PROCEDURE: SI-2.1

Assessment Objective

Determine if:
(i) the organization identifies, reports, and corrects information system flaws;

(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;

(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;

(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation;

(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST Special Publication 800-40; 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

Updates are installed automatically.

Applicability: All	**Reference(s):** ARS: SI-2(1); 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 and installs 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

Employ automated mechanisms periodically and upon demand to determine the state of information system components with regard to flaw remediation.

Applicability: All	**Reference(s):** ARS: SI-2(2); 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

Determine if the organization employs automated mechanisms to periodically and upon demand 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.

Test: Automated mechanisms implementing information system flaw remediation update status.

SI-3 – Malicious Code Protection (High)

Control

Automated malicious code protection mechanisms that include a capability of automatic updates shall be in place and supporting procedures shall be developed, documented, and implemented effectively to identify and isolate suspected malicious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical information system entry points, and at each workstation, server, or mobile computing device on the network to detect and eradicate malicious code transported by email, email attachments, removable media or other methods. Business Owners shall use antiviral software products from multiple vendors, if possible, and update virus protection mechanisms whenever new releases are available.

Implementation Standard(s)

1. Implement malicious code protection at information system entry points, including firewalls, email servers, remote access servers, workstations, servers, and mobile computing devices by employing automated mechanisms to detect and eradicate malicious code transported by email, email attachments, and removable media.
2. Enable real-time file scanning. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and every twelve (12) hours.

Guidance

The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and

procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST SP 800-83 provides guidance on implementing malicious code protection.

Applicability: All	**Reference(s):** ARS: SI-3; FISCAM: CM-5; IRS-1075: 5.6.2.5#1.3; PISP: 4.17.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-3.1

Assessment Objective

Determine if the information system implements malicious code protection by verifying that:
- the organization employs malicious code protection mechanisms at critical information system entry and exit points, and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;
- the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities;
- the organization updates malicious code protection mechanisms whenever new releases are available, to include the latest malicious code definitions, in accordance with organizational configuration management policy and procedures;
- the organization considered use of malicious code protection software products from multiple vendors;
- the organization considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST Special Publication 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

Test: Malicious code protection capability.

SI-3(1) – Enhancement (High)

Control

Manage and update malicious code protection software centrally with automatic updates for the latest malicious code definitions whenever new releases are available.

Applicability: All	**Reference(s):** ARS: SI-3(1); 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

Employ automated mechanisms to update malicious code protection.

Applicability: All	**Reference(s):** ARS: SI-3(2); IRS-1075: 5.6.2.5#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-3(2).1

Assessment Objective

Determine if the organization automatically updates 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-4 – Information System Monitoring Tools and Techniques (High)

Control

Effective monitoring tools and techniques providing real-time identification of unauthorized use, misuse, and abuse of the information system shall be implemented.

Implementation Standard(s)

1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.

Guidance

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). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST SP 800-61 provides guidance on detecting attacks through various types of security technologies. NIST SP 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST SP 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST SP 800-94 provides guidance on intrusion detection and prevention.

Applicability: All	**Reference(s):** ARS: SI-4; 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; PISP: 4.17.4	**Related Controls Requirement(s):** AC-8, AU-4, CM-6

ASSESSMENT PROCEDURE: SI-4.1

Assessment Objective

Determine if:

(i) the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system;

(ii) the organization deploys monitoring devices strategically within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information;

(iii) the organization deploys monitoring devices at ad hoc locations within the information system to track specific transactions;

(iv) the organization uses the monitoring devices to track the impact of security changes to the information system;

(v) the organization determines the granularity of the information collected based upon its monitoring objectives and the capability of the information system to support such activities;

(vi) the organization consults appropriate legal counsel with regard to all information system monitoring activities;

(vii) the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation, based on law enforcement information, intelligence information, or other credible sources of information.

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 (High)		
Control Connect individual IDS devices to a common IDS management network using common protocols.		
Applicability: All	**Reference(s):** ARS: SI-4(1); 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 systemwide 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 Employ automated information system monitoring tools to support near-real-time analysis of events.		
Applicability: All	**Reference(s):** ARS: SI-4(2)	**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 Employ automated tools to integrate intrusion detection tools into access control mechanisms to enable rapid response to attacks through the re-configuration of IDS settings to support attack isolation and elimination.		
Applicability: All	**Reference(s):** ARS: SI-4(3)	**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

Monitor inbound and outbound communications for unusual or unauthorized activities or conditions.

Guidance

Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.

Applicability: All	**Reference(s):** ARS: SI-4(4); 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

Determine if:
(i) the organization identifies the types of activities or conditions considered unusual or unauthorized;

(ii) 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; types of activities or conditions considered unusual or unauthorized; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system monitoring capability for inbound and outbound communications.

SI-4(5) – Enhancement (High)

Control

Real-time alerts are provided when indications of the following types 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.

Applicability: All	**Reference(s):** ARS: SI-4(5)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-4(5).1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, indications of compromise or potential compromise to the security of the information system;

(ii) the information system provides a real-time alert 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; System Security Plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system monitoring real-time alert capability.

SI-5 – Security Alerts and Advisories (High)

Control

Procedures shall be developed, documented, and implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis, and for issuing IS alerts and advisories to appropriate personnel. Upon receipt of such alerts and advisories, personnel shall take appropriate response actions. The types of actions to be taken in response to security alerts / advisories shall be documented.

Guidance

The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST SP 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Applicability: All	**Reference(s):** ARS: SI-5; FISCAM: AC-5, AS-3, CM-5, DA-1, SM-5; PISP: 4.17.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-5.1

Assessment Objective

Determine if:
(i) the organization receives information system security alerts/advisories on a regular basis;

(ii) the organization issues security alerts/advisories to appropriate organizational personnel;

(iii) the organization takes appropriate actions in response to security alerts/advisories;

(iv) the organization maintains contact with special interest groups (e.g., information security forums) that:
- facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies);
- provide access to advice from security professionals;
- improve knowledge of security best practices.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; NIST Special Publication 800-40; 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

Employ automated mechanisms to make security alerts and advisory information available to all appropriate personnel.

Applicability: All	**Reference(s):** ARS: SI-5(1)	**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 as needed.

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

Automated mechanisms shall be established and implemented effectively to provide the capability for CMS information systems to verify the correct operation of security functions on a regular basis, and automatically to take appropriate response actions when security-related anomalies are discovered.

Implementation Standard(s)

1. Configure the information system to automatically verify the correct operation of system security functions upon system startup and restart, upon command by users with appropriate access, and at least on a monthly routine basis and to notify system administration upon detection of security anomalies.

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 either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Applicability: All	**Reference(s):** ARS: SI-6; FISCAM: AC-5, CM-4; PISP: 4.17.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-6.1

Assessment Objective

Determine if:
(i) the organization defines in the System Security Plan, explicitly or by reference, the appropriate conditions for conducting security function verification;

(ii) the organization defines in the System Security Plan, explicitly or by reference, for periodic security function verification, the frequency of the verifications;

(iii) the organization defines in the System Security Plan, explicitly or by reference, information system responses to anomalies discovered during security function verification;

(iv) 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);

(v) the information system responds to security function anomalies in accordance with organization-defined responses.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; System 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

Employ automated mechanisms to provide centralized notification of failed automated security tests.

Applicability: All	**Reference(s):** ARS: SI-6(1)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-6(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to provide notification of failed security tests.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; System Security Plan; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing alerts and/or notifications for failed automated security tests.

SI-6(2) – Enhancement (High)

Control

Employ automated mechanisms to support centralized management of distributed security testing.

Applicability: All	**Reference(s):** ARS: SI-6(2)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-6(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to support management of distributed security testing.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; System 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

Automated mechanisms for software and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to software. Good software engineering practices consistent with CMS IS policy and procedures shall be employed 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.

Implementation Standard(s)

1. Employ off-the-shelf integrity mechanisms such as 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 and use tools to automatically monitor the integrity of the information system and the application it hosts.

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 with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Applicability: All	**Reference(s):** ARS: SI-7; FISCAM: AC-4, CM-4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); PISP: 4.17.7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-7.1

Assessment Objective

Determine if:
(i) the information system detects and protects against unauthorized changes to software and information;

(ii) the organization employs commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) in accordance with good software engineering practices and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

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 Perform weekly integrity scans of the system.		
Applicability: All	**Reference(s):** ARS: SI-7(1); HIPAA: 164.312(c)(2), 164.312(e)(2)(i)	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SI-7(1).1		
Assessment Objective Determine if: (i) the organization defines in the System Security Plan, explicitly or by reference, the frequency of integrity scans on the information system; (ii) 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; System 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 Employ automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.		
Applicability: All	**Reference(s):** ARS: SI-7(2); HIPAA: 164.312(c)(2), 164.312(e)(2)(i)	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SI-7(2).1		
Assessment Objective Determine if the organization employs automated tools that provide notification to appropriate 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 Automated mechanisms for spam protection shall be in place at critical information system entry points, workstations, servers, and mobile computing devices on the network. Supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect spam.		
Guidance The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST SP 800-45 provides guidance on electronic mail security.		
Applicability: All	**Reference(s):** ARS: SI-8; FISCAM: CM-5; HIPAA: 164.308(a)(1)(i); PISP: 4.17.8	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-8.1

Assessment Objective

Determine if the information system implements spam protection by verifying that the organization:
- employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network;
- employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means.

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: Spam detection and handling capability.

SI-8(1) – Enhancement (High)

Control

Centrally manage spam protection mechanisms.

Applicability: All	**Reference(s):** ARS: SI-8(1); 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

Automatically update spam protection mechanisms.

Applicability: All	**Reference(s):** ARS: SI-8(2); 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.

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

Automated mechanisms shall be in place to restrict information input to the information system to authorized personnel. Personnel authorized to input information to the information system shall be restricted beyond the typical access controls employed by the system, including limitations based on specific operational / project responsibilities.

Guidance

Restrictions on 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):** ARS: SI-9; 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; PISP: 4.17.9	**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 Accuracy, Completeness, Validity, and Authenticity (High)

Control

Automated mechanisms shall verify information for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

Implementation Standard(s)

1. Implement automated system checks of information for accuracy, completeness, validity, and authenticity.

Guidance

Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax 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. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Applicability: All	**Reference(s):** ARS: SI-10; FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; IRS-1075: 5.6.2.5#1.1-2; PISP: 4.17.10	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-10.1

Assessment Objective

Determine if the information system checks information for accuracy, completeness, validity, and authenticity by verifying that the system:
- checks for accuracy, completeness, validity, and authenticity of information is accomplished as close to the point of origin as possible;
- employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions for format and content;
- prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands;
- checks the accuracy, completeness, validity, and authenticity of information to the extent guided by organizational policy and operational requirements.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system capability for checking information for accuracy, completeness, validity, and authenticity.

SI-11 – Error Handling (High)

Control

Information systems shall identify and handle error conditions in an expeditious manner. User error messages generated by information systems shall provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages shall be revealed only to authorized personnel. Sensitive information shall not be listed in error logs or associated administrative messages.

Implementation Standard(s)

1. Employ automated mechanisms that generate error messages providing timely and useful information to users without revealing information that could be exploited by adversaries. Ensure confidential information (e.g., account numbers, User IDs, social security numbers, etc.) is not listed in error logs or associated with administrative messages.

Guidance

The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Applicability: All	**Reference(s):** ARS: SI-11; FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; PISP: 4.17.11	**Related Controls Requirement(s):** SI-2

ASSESSMENT PROCEDURE: SI-11.1

Assessment Objective

Determine if:
(i) the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries;

(ii) the information system reveals error messages only to authorized individuals;

(iii) the information system does not include sensitive information in error logs or associated administrative messages.

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

Output from information systems shall be handled and retained in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, operational requirements, and the information sensitivity level.

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

A good place to obtain procedures for handling sensitive output information is the NIST SP.

Applicability: All	**Reference(s):** ARS: SI-12; FISCAM: BP-2, BP-3; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2; PISP: 4.17.12	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-12.1
Assessment Objective
Determine if: (i) the organization handles output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; (ii) the organization retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
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.