

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

## **Appendix C - CMSR Low Impact Level Data**

*(Rev. 2, Issued: 03-07-14)*

### **Table of Contents**

1.0	Access Control (AC)	2
2.0	Awareness and Training (AT)	25
3.0	Audit and Accountability (AU)	31
4.0	Security Assessment and Authorization (CA)	43
5.0	Configuration Management (CM)	56
6.0	Contingency Planning (CP)	68
7.0	Identification and Authentication (IA)	79
8.0	Incident Response (IR)	94
9.0	Maintenance (MA)	103
10.0	Media Protection (MP)	109
11.0	Physical and Environmental Protection (PE)	115
12.0	Planning (PL)	126
13.0	Personnel Security (PS)	132
14.0	Risk Assessment (RA)	143
15.0	System and Services Acquisition (SA)	150
16.0	System and Communications Protection (SC)	160
17.0	System and Information Integrity (SI)	172
18.0	<i>Program Management (PM)</i>	187

19.0	<i>Authority and Purpose (AP)</i>	203
20.0	<i>Accountability, Audit, and Risk Management (AR)</i>	206
21.0	<i>Data Quality and Integrity (DI)</i>	215
22.0	<i>Data Minimization and Retention (DM)</i>	218
23.0	<i>Individual Participation and Redress (IP)</i>	222
24.0	<i>Security (SE)</i>	227
25.0	<i>Transparency (TR)</i>	230
26.0	<i>Use Limitation (UL)</i>	234

## 1.0 ACCESS CONTROL (AC)

*(Rev. 2, Issued: 03-07-14, Effective: 04-07-14, Implemented: 03-09-15, 10-06-14-VMS to Implement the Client Letter Work)*

AC-1 – Access Control Policy and Procedures (Low)	Assurance - PI
<p><b>Control</b></p> <p>The organization:</p> <ul style="list-style-type: none"> <li><i>a. Develops, documents, and disseminates to applicable personnel:</i> <ul style="list-style-type: none"> <li><i>1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the access control policy and associated access controls; and</i></li> </ul> </li> <li><i>b. Reviews and updates the current:</i> <ul style="list-style-type: none"> <li><i>1. Access control policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. Access control procedures within every three hundred sixty-five (365) days.</i></li> </ul> </li> </ul> <p><b>Guidance</b></p> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>AC</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain</i></p>	

*organizations. The* procedures can be *established* for the security program in general and for particular information *systems, if needed*. The organizational risk management strategy is a key factor in *establishing* policy *and procedures*.

**Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(1); IRS-1075: 9.2#1; NIST SP: 800-12, 800-100

**Related Controls Requirement(s):** PM-9

## ASSESSMENT PROCEDURE: AC-1.1

### Assessment Objective

Determine if:

(i) the organization develops and documents access control policy;

(ii) the organization access control policy addresses:

- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented access control policy to *applicable personnel* within the organization having associated access control roles and responsibilities;

(iv) the organization develops and documents access control procedures;

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

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

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

### Assessment Methods And Objects

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

## AC-2 – Account Management (Low)

*PI*

### Control

The organization:

*a. Identifies and selects the following types of* information system accounts

*to support organizational missions/business functions:* individual, group, system, application, guest/anonymous, *emergency*, and temporary;

b. *Assigns account managers for information system accounts;*

c. *Establishes* conditions for group *and role* membership;

d. *Specifies* authorized users of the information system, *group* and *role membership, and* access *authorizations (i.e., privileges) and other attributes (as required) for each account;*

e. *Requires* approvals *by account managers* for requests to create information system accounts;

f. *Creates, enables, modifies, disables, and removes information system accounts in accordance with ARS requirements and Risk Management Handbook (RMH) Standards and Procedures;*

g. *Monitors the use of, information system accounts;*

h. *Notifies* account managers:

1. *When* accounts are no longer required;

2. *When* users are terminated *or* transferred; *and*

3. *When individual* information system usage or need-to-know changes;

i

. *Authorizes* access to the *information* system based on:

1. A valid access authorization;

2. Intended system usage; and

3. Other attributes as required by the organization or associated missions/business functions;

j. Review *s* accounts *for compliance with account management requirements* using the frequency specified in Implementation Standard 1; *and*

k. *Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.*

#### **Implementation Standard(s)**

1. Review information system accounts within every three hundred sixty-five (365) days and require annual certification.

2. Remove or disable default user accounts. Rename active default accounts.

3. Implement centralized control of user access administrator functions.

4. Regulate the access provided to contractors and define security requirements for contractors.

5. *(For CSP only) For service providers, the organization reviews information system accounts and requires certification at least annually.*

## Guidance

*Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training.*

**Reference(s):** FISCAM: AC-3, AS-2; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii); IRS-1075: 5.3#3, 9.2#2.1, 9.2#2.3-end

**Related Controls Requirement(s):** AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, CM-5, CM-6, CM-11, IA-2, IA-4, IA-5, IA-8, MA-3, MA-4, MA-5, PL-4, SC-13

## ASSESSMENT PROCEDURE: AC-2.1

### Assessment Objective

Determine if:

- (i) the organization manages information system accounts, including;
  - identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
  - establishing conditions for group membership;

- identifying authorized users of the information system and specifying access privileges;
- requiring appropriate approvals for requests to establish accounts;
- establishing, activating, modifying, disabling, and removing accounts;
- specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
- *authorizes* access to the system based on: (a) a valid access authorization; (b) intended system usage; and (c) other attributes as required by the organization or associated missions/business functions;
- (ii) the organization reviews information system accounts in accordance with the frequency specified in Implementation Standard 1;
- (iii) *the organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.*
- (iv) *the organization meets all the requirements specified in the applicable Implementation Standard(s).*

#### Assessment Methods And Objects

**Examine:** Access control policy; procedures addressing account management; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest/anonymous and temporary accounts along with the name of the individual associated with the each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.

#### AC-2(3) - *Disable Inactive Accounts* – Enhancement (Low)

*P1*

#### Control

The information system automatically disables inactive accounts *within* three hundred sixty-five (365) days.

#### *Implementation Standard(s)*

*1. (For CSP only) AC-2(3) is not required at Low level for FedRAMP-authorized service providers.*

**Reference(s):** *IRS-1075: 9.2#2.1*

**Related Controls Requirement(s):**

#### ASSESSMENT PROCEDURE: AC-2(3).1

#### Assessment Objective

Determine if:

(i) the organization defines in the 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; security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records.

### AC-3 – Access Enforcement (Low)

**PI**

#### Control

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

#### Implementation Standard(s)

1. *If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13).*
2. *Configure operating system controls to disable public "write" access to files, objects, and directories that may directly impact system functionality and/or performance.*

#### Guidance

Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between *active entities or subjects* (i.e., users or processes acting on behalf of users) and *passive entities or* objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level *and recognizing that information systems can host many applications and services in support of organizational missions and business operations*, access enforcement mechanisms *can also be* employed at the application *and service* level to provide increased information security. *For minimum authentication requirements, refer to Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.*

**Reference(s):** FISCAM: AC-3, AS-2; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv); IRS-1075: 9.2 #2.2, 9.3#3

**Related Controls Requirement(s):** AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3

<b>ASSESSMENT PROCEDURE: AC-3.1</b>	
<b>Assessment Objective</b> Determine if: <i>(i)</i> the information system enforces approved authorizations for logical access to the system in accordance with applicable policy. <i>(ii)</i> the organization meets all the requirements specified in the applicable Implementation Standard(s).	
<b>Assessment Methods And Objects</b> <b>Examine:</b> Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records.	
<b>AC-5 – Separation of Duties (Low)</b>	
<b>Control</b>	
The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion; b. Documents separation of duties; and c. <i>Defines</i> information system access authorizations <i>to support separation of duties</i> .	
<b>Implementation Standard(s)</b> 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. <i>7. (For CSP only) AC-5 is not required at Low level for FedRAMP-authorized service providers.</i>	
<b>Guidance</b>	
Separation of duties <i>addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example:</i> (i) <i>dividing</i> mission functions and information system support functions among different individuals <i>and/or</i> roles; (ii) <i>conducting</i> information system support functions <i>with different individuals</i> (e.g., system management, programming, configuration management, quality assurance and testing, <i>and</i> network security); <i>and</i> (iii) <i>ensuring</i> security personnel <i>administering</i> access control functions do not <i>also</i> administer audit functions.	
<b>Reference(s):</b> FISCAM: AS-4, SD-1, SD-2; HIPAA: 164.308(a)(3)(i), <i>164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.312(a)(1)</i> ; IRS-1075: <i>9.2#4.1, 9.3#3, 9.6#1</i>	<b>Related Controls Requirement(s):</b> <i>AC-3, AC-6, PE-3, PE-4, PS-2</i>



<b>ASSESSMENT PROCEDURE: AC-5.1</b>	
<b>Assessment Objective</b> Determine if: <i>(i)</i> the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion; <i>(ii)</i> the organization documents separation of duties; <i>(iii)</i> the organization <i>defines</i> information system access authorizations <i>to support separation of duties</i> . <i>(iv)</i> the organization meets all the requirements specified in the applicable Implementation Standard(s).	
<b>Assessment Methods And Objects</b> <b>Examine:</b> 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.	
<b>AC-6 – Least Privilege (Low)</b>	
<b>PI</b>	
<b>Control</b> The organization employs the <i>principle</i> of least privilege, allowing only authorized accesses for users ( <i>or</i> processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with CMS missions and business functions.	
<b>Implementation Standard(s)</b> 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. 5. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If <i>system and removable media boot access is</i> authorized, boot access is password protected. 6. <i>(For CSP only) AC-6 is not required at Low level for FedRAMP-authorized service providers.</i>	
<b>Guidance</b> <i>Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.</i>	
<b>Reference(s):</b> FISCAM: AC-3, AS-2; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(i),	<b>Related Controls Requirement(s):</b> AC-2,

<i>164.308(a)(4)(ii)(A), 164.312(a)(1); HSPD 7: D(10); IRS-1075: 9.2 #4.2, 9.6#1</i>	<i>AC-3, AC-5, CM-6, CM-7, PL-2</i>
<b>ASSESSMENT PROCEDURE: AC-6.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <p>(i) the organization employs the <i>principle</i> of least privilege, allowing only authorized accesses for users (<i>or</i> processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.</p> <p>(ii) the organization meets all the requirements specified in the applicable Implementation Standard(s).</p> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> 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.</p>	
<b>AC-6(1) - <i>Authorize Access to Security Functions</i> – Enhancement (Low)</b>	
<p><b>Control</b></p> <p><i>At a minimum</i>, the organization explicitly authorizes access to <i>the following list of security</i> functions (deployed in hardware, software, and firmware) and security-relevant information:</p> <ul style="list-style-type: none"> <li>- <i>Setting/modifying audit logs and auditing behavior;</i></li> <li>- <i>Setting/modifying boundary protection system rules;</i></li> <li>- <i>Configuring/modifying access authorizations (i.e., permissions, privileges);</i></li> <li>- <i>Setting/modifying authentication parameters; and</i></li> <li>- <i>Setting/modifying system configurations and parameters.</i></li> </ul> <p><b>Implementation Standard(s)</b></p> <p><i>1. (For CSP only) AC-6(1) is not required at Low level for FedRAMP-authorized service providers.</i></p>	
<p><b>Guidance</b></p> <p><i>Security functions include, for example</i>, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. <i>Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.</i> Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.</p>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s):</b> <i>AC-17,</i>

		AC-18, AC-19
<b>ASSESSMENT PROCEDURE: AC-6(1).1</b>		
<b>Assessment Objective</b> Determine if: (i) the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; (ii) the organization explicitly authorizes access to the organization-defined security functions and security-relevant information.		
<b>Assessment Methods And Objects</b> <b>Examine:</b> Access control policy; procedures addressing least privilege; list of security functions and security-relevant information for which access must be explicitly authorized; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		
<b>AC-6(2) - Non-Privileged Access for Nonsecurity Functions – Enhancement (Low)</b>		<b>PI</b>
<b>Control</b> <i>At a minimum</i> , the organization requires that users of information system accounts, or roles, with access to <i>the following list of security functions</i> or <i>security-relevant information</i> , use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions: - <i>Setting/modifying audit logs and auditing behavior;</i> - <i>Setting/modifying boundary protection system rules;</i> - <i>Configuring/modifying access authorizations (i.e., permissions, privileges);</i> - <i>Setting/modifying authentication parameters; and</i> - <i>Setting/modifying system configurations and parameters.</i> <b>Implementation Standard(s)</b> 1. <i>(For CSP only) AC-6(2) is not required at Low level for FedRAMP-authorized service providers.</i>		
<b>Guidance</b> This control enhancement <i>limits</i> exposure <i>when</i> operating from within privileged accounts or roles. The inclusion of <i>roles addresses</i> situations where <i>organizations implement</i> access control policies such as <i>role-based access control</i> and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.		
<b>Reference(s):</b>		<b>Related Controls Requirement(s): PL-4</b>

## ASSESSMENT PROCEDURE: AC-6(2).1

### Assessment Objective

Determine if:

- (i) the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access;
- (ii) the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions;
- (iii) the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions.

### Assessment Methods And Objects

**Examine:** Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

## AC-7 – Unsuccessful Login Attempts (Low)

P2

### Control

The information system:

- a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and
- b. Automatically disables or locks the account/node until released *by an administrator or* after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded.

### Implementation Standard(s)

1. Configure the information system to disable access for at least five (5) minutes after three (3) *invalid login attempts during a five (5) minute time period.*
2. *(For CSP only) For service providers, the information system:*
  - a. *Enforces a limit of not more than three (3) consecutive invalid login attempts by a user during a fifteen (15) minute time period; and*
  - b. *Automatically locks the account/node for thirty (30) minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.*

### Guidance

*This control applies regardless of whether the login occurs via a local or network connection.* Due to the potential for denial of

service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

**Reference(s):** FISCAM: AC-2, AS-2; IRS-1075: 9.2#5

**Related Controls Requirement(s):** AC-2, AC-9, AC-14, IA-5

## ASSESSMENT PROCEDURE: AC-7.1

### Assessment Objective

Determine if:

- (i) the organization defines in the security plan, explicitly or by reference, the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid login attempts occur;
- (ii) the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period;
- (iii) the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:
  - lock out the account/node for a specified time period;
  - lock out the account/node until released by an administrator; or
  - delay the next login prompt according to organization-defined delay algorithm;
- (iv) the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded;
- (v) the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded.
- (vi) the organization meets all the requirements specified in the applicable Implementation Standard(s).

### Assessment Methods And Objects

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

## AC 8 – System Use Notification (Low)

**PI**

### Control

The information system:

a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner *states*:

- You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

- By using this information system, you understand and consent to the following:

- \* You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

- \* Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems:

1. *Displays* system use information when appropriate, before granting further access;

2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. *Includes* a description of the authorized uses of the system.

***Implementation Standard(s)***

1. *(For CSP only) For service providers, the organization determines elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Joint Authorization Board (JAB).*

2. *(For CSP only) For service providers, the organization determines how System Use Notification is going to be verified and provides appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the Joint Authorization Board (JAB).*

3. *(For CSP only) For service providers, if not performed as part of a Configuration Baseline check, the organization has a documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the Joint Authorization Board (JAB).*

### Guidance

The warning banner language has very important legal implications for CMS and its information system resources. Should content need to be added to this banner, submit the modified warning banner language to the CMS CIO for review and approval prior to implementation. If an information system has character limitations related to the warning banner display, the CMS CIO can provide an abbreviated warning banner version. If this banner is inconsistent with any directives, policies, regulations, or standards, notify the CMS CIO immediately.

All information system computers and network devices under CMS control, prominently display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web sites, web pages where substantial personal information from the public is collected, *sftp, SSH*, or other services accessed.

System use *notifications* can be implemented *using messages or* warning banners displayed *before* individuals log in to information systems. System use *notifications are used* only for access *via logon interfaces* with human users and *are* not *required when such human interfaces do* not exist.

*(For CSP only) If performed as part of the service provider Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.*

**Reference(s):** FISCAM: AC-1, *AS-2*; IRS-1075: 5.1#1.3, *9.2#6*

**Related Controls Requirement(s):**

### ASSESSMENT PROCEDURE: AC-8.1

#### Assessment Objective

Determine if:

*(i)* the information system displays the CMS-approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

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

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

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

*(iv) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

### Assessment Methods And Objects

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

### ASSESSMENT PROCEDURE: AC-8.2

#### Assessment Objective

Determine if:

- (i) the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access;
- (ii) the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities;
- (iii) the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.

#### Assessment Methods And Objects

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

### AC-14 – Permitted Actions Without Identification or Authentication (Low)

**PI**

#### Control

The organization:

- a. *Identifies specific user actions that can be performed on the information system without identification or authentication;*
- b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification *or* authentication; and
- c. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

#### Guidance

This control *addresses situations in which organizations determine* that no identification *or* authentication is required *in organizational information systems. Organizations* may allow a limited number of user actions without identification *or* authentication *including, for example*, when individuals access public websites or other publicly accessible federal information



systems, *when individuals use mobile phones to receive calls, or when facsimiles are received*. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may *occur*, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. *Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none.*

Reference(s): FISCAM: AC-2, AS-2

Related Controls Requirement(s): *CP-2, IA-2*

#### ASSESSMENT PROCEDURE: AC-14.1

##### Assessment Objective

Determine if:

- (i)* the organization identifies specific user actions that can be performed on the information system without identification or authentication;
- (ii)* the organization documents *or* provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

##### Assessment Methods And Objects

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

#### AC-17 – Remote Access (Low)

*PI*

##### Control

*The organization monitors for unauthorized remote access to the information system.* Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If *remote access is* authorized, the organization:

a.

Establishes *and documents* usage restrictions, *configuration/connection requirements*, and implementation guidance for each *type of* remote access *allowed; and*

*b.* Authorizes remote access to the information system prior to *allowing such* connections.

**Implementation Standard(s)**

1. Require callback capability with re-authentication to verify connections from authorized locations when the *CMS Net* or Multi Protocol Label Switching (MPLS) service network cannot be used.
2. *All computers and devices, whether government-furnished equipment (GFE) or contractor-furnished equipment (CFE), that require any network access to a network or system are securely configured and meet at least the following security requirements: (i) up-to-date system patches, and (ii) current anti-virus software; and (iii) functionality that provides the capability for automatic execution of code disabled.*

**Guidance**

Remote access is access to *organizational* information systems by *users* (or processes acting on behalf of *users*) communicating through external networks (e.g., the Internet). Remote access methods include, *for example*, dial-up, broadband, and wireless. *Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs, does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code.* Remote access controls *apply* to information systems other than public web servers or systems designed for public access. *This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control.* Enforcing access restrictions *for* remote connections is *addressed in AC-3.*

*For minimum authentication requirements, refer to Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.*

**Reference(s):** FISCAM: AC-1, *AS-2*; HIPAA: 164.310(b); IRS-1075: 9.2#10, 9.18.3 #1, 9.18.3#2; NIST SP: 800-46, 800-77, 800-113, 800-114, 800-121

**Related Controls Requirement(s):** AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4

**ASSESSMENT PROCEDURE: AC-17.1**

**Assessment Objective**

*Determine if:*

(i) the organization establishes *and documents* usage restrictions, *configuration/connection requirements*, and implementation guidance for each allowed *type of* remote access method *allowed*;

- (ii) the organization monitors for unauthorized remote access to the information system;
- (iii) the organization authorizes remote access to the information system prior to *allowing such connections*;
- (iv) the organization meets all the requirements specified in the applicable Implementation Standard(s).

#### Assessment Methods And Objects

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

#### AC-17(7) - *Additional Protection for Security Function Access* – Enhancement (Low)

*PI*

#### Control

*[Withdrawn: Incorporated into AC-3].*

#### AC-18 – Wireless Access (Low)

*PI*

#### Control

The organization *monitors for unauthorized wireless access to information systems and* prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If *wireless access is* authorized, the organization *establishes usage restrictions, configuration/connection requirements, and implementation guidance* for wireless *access prior to allowing such* connections.

#### Implementation Standard(s)

1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless *restrictions and* access controls are implemented:
  - (a) Encryption protection is enabled;
  - (b) Access points are placed in secure areas;
  - (c) Access points are shut down when not in use (i.e., nights, weekends);
  - (d) A firewall is implemented between the wireless network and the wired infrastructure;
  - (e) MAC address authentication is utilized;
  - (f) Static IP addresses, not DHCP, is utilized;
  - (g) Personal firewalls are utilized on all wireless clients;
  - (h) File sharing is disabled on all wireless clients;
  - (i) Intrusion detection agents are deployed on the wireless side of the firewall;
  - (j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis; *and*
  - (k) *Adheres to CMS-CIO-POL-INF12-01, CMS Policy for Wireless Client Access.*

<b>Guidance</b> Wireless technologies include, <i>for example</i> , microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.	
<b>Reference(s):</b> FISCAM: AC-1, <i>AS-2; IRS-1075: 9.2#11; NIST SP: 800-48, 800-94, 800-97</i>	<b>Related Controls Requirement(s):</b> <i>AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4</i>
<b>ASSESSMENT PROCEDURE: AC-18.1</b>	
<b>Assessment Objective</b> Determine if: <i>(i)</i> the organization establishes usage restrictions and implementation guidance for wireless access; <i>(ii)</i> the organization monitors for unauthorized wireless access to information systems; <i>(iii)</i> the organization authorizes wireless access to the information system prior to connection; <i>(iv)</i> the organization <i>establishes usage restrictions, configuration/connection requirements, and implementation guidance</i> for wireless <i>access prior to allowing such</i> connections. <i>(v)</i> the organization meets all the requirements specified in the applicable Implementation Standard(s).	
<b>Assessment Methods And Objects</b> <b>Examine:</b> Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records.	
<b>AC-19 – Access Control for Mobile Devices (Low)</b>	
<b>Control</b> <i>The organization:</i> <i>a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and</i> <i>b. CIO authorizes</i> the connection of mobile devices to <i>organizational</i> information systems. <b>Implementation Standard(s)</b> <i>1. (For CSP only) For service providers, the organization defines inspection and preventative measures. The measures are approved and accepted by Joint Authorization Board (JAB).</i>	

## Guidance

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

**Reference(s):** FISCAM: AC-1, AS-2; HIPAA: 164.310(b); IRS-1075: 4.6#1, 4.7.1#2, 9.2#12; NIST SP: 800-114, 800-124, 800-164; OMB: M-06-16

**Related Controls Requirement(s):** AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4

## ASSESSMENT PROCEDURE: AC-19.1

### Assessment Objective

Determine if:

- (i) the organization prohibits the connection of portable and mobile devices to the information system unless explicitly authorized, in writing, by the CIO;*
- (ii) the organization monitors for unauthorized connections of mobile devices to organizational information systems;*
- (iii) if authorized, the organization establishes usage restrictions, connection requirements, and implementation guidance for organization-controlled mobile devices;*

*(iv) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

### Assessment Methods And Objects

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

### AC-20 – Use of External Information Systems (Low)

**PI**

#### Control

The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. *If external information systems are* authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall address, at a minimum:

- a. The types of applications that can be accessed from external information systems;
- b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
- c. How other users of the external information system will be prevented from accessing federal information;
- d. The use of virtual private networking (VPN) and firewall technologies;
- e. The use of and protection against the vulnerabilities of wireless technologies;
- f. The maintenance of adequate physical security controls;
- g. The use of virus and spyware protection software; and
- h. How often the security capabilities of installed software are to be updated.

#### Implementation Standard(s)

1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.

#### Guidance

External information systems are information systems or components of information systems that are outside of the authorization boundary established by *organizations* and for which *organizations* typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, *for example*: (i) personally owned information systems/*devices* (e.g., *notebook* computers, *smart phones*, *tablets*, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, *train stations*, convention centers, *shopping malls*, or airports); (iii) information systems owned or controlled by nonfederal

governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of *organizations*. *This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.*

*For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.*

*This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.medicare.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.*

For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to CMS, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external.

**Reference(s):** *FIPS Pub: 199; FISCAM: AS-1, SM-7; IRS-1075: 4.7.1#1, 4.7.2#1, 4.7.3#1.1, 9.18.2#2*

**Related Controls Requirement(s):** *AC-3, AC-17, AC-19, CA-3, PL-4, SA-9*

#### **ASSESSMENT PROCEDURE: AC-20.1**

##### **Assessment Objective**

Determine if:

*(i)* the organization prohibits the use of external information systems to store, access, transmit, or process sensitive information



unless explicitly authorized, in writing, by the CIO;

(ii) if authorized, the organization identifies individuals authorized to:

- access the information system from the external information systems;
- process, store, and/or transmit organization-controlled information using the external information systems;

(iii) if authorized, the terms and conditions address, at a minimum:

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

(iv) the organization meets all the requirements specified in the applicable Implementation Standard(s).

#### Assessment Methods And Objects

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

#### AC-22 – Publicly Accessible Content (Low)

P2

#### Control

The organization:

- a. Designates individuals authorized to post information onto a *publicly accessible* information system;
- b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- c. Reviews the proposed content of *information prior to posting onto the* publicly accessible information *system to ensure that* nonpublic information *is not included; and*
- d. Reviews the content on the publicly accessible information system for nonpublic information *bi-weekly* and *removes such* information, if discovered.

#### Implementation Standard(s)

*1. (For CSP only) For service providers, the organization reviews the content on the publicly accessible organizational information system for nonpublic information at least quarterly.*



<b>Guidance</b> <p>In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, <i>and/or</i> guidance, <i>the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information).</i> This control addresses information <i>systems</i> that <i>are controlled by the organization and</i> accessible to the general public, typically without identification or authentication. The posting of information on non-CMS information systems is covered by organizational policy.</p>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s):</b> <i>AC-3, AC-4, AT-2, AT-3, AU-13</i>
<b>ASSESSMENT PROCEDURE: AC-22.1</b>	
<b>Assessment Objective</b> <p>Determine if:</p> <ul style="list-style-type: none"> <li><i>(i) the organization designates individuals authorized to post information onto a <b>publicly accessible</b> information system that is publicly accessible;</i></li> <li><i>(ii) the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;</i></li> <li><i>(iii) the organization reviews the proposed content of <b>information prior to posting onto the</b> publicly accessible information <b>system to ensure that</b> nonpublic information <b>is not included</b>;</i></li> <li><i>(iv) the organization reviews the content on the publicly accessible information system for nonpublic information <b>in accordance with the organization-defined time period</b>;</i></li> <li><i>(v) the organization removes nonpublic information, if discovered.</i></li> <li><i>(vi) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul>	
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records; other relevant documents or records.</p>	

## 2.0 AWARENESS AND TRAINING (AT)

*Error! Reference source not found.*

AT-1 – Security Awareness and Training Policy and Procedures (Low)	Assurance - P1
<p><b>Control</b></p> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li>1. A security <i>and privacy</i> awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the security <i>and privacy</i> awareness and training policy and associated security <i>and privacy</i> awareness and training controls; and</li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li>1. Security and privacy awareness and training policy within every three hundred sixty-five (365) days; and</li> <li>2. Security and privacy awareness and training procedures within every three hundred sixty-five (365) days.</li> </ol>	
<p><b>Guidance</b></p> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>AT</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing policy and procedures</i>.</p>	
<p><b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; <i>HIPAA: 164.308(a)(5)(i); IRS-1075: 6.1#1, 9.4#1.1; NIST SP: 800-12, 800-16, 800-50, 800-100</i></p>	<p><b>Related Controls Requirement(s):</b> <i>PM-9</i></p>
<p><b>ASSESSMENT PROCEDURE: AT-1.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ol style="list-style-type: none"> <li>(i) the organization develops and documents <i>a</i> security <i>and privacy</i> awareness and training policy;</li> <li>(ii) the organization security <i>and privacy</i> awareness and training policy addresses: <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> </ul> </li> </ol>	

- roles and responsibilities;
- management commitment;
- coordination among organizational entities, and compliance;

(iii) the organization disseminates documented security *and privacy* awareness and training policy to *applicable personnel* within the organization having associated security *and privacy* awareness and training roles and responsibilities;

(iv) the organization develops and documents security *and privacy* awareness and training procedures;

(v) the organization security *and privacy* awareness and training procedures facilitate implementation of the security *and privacy* awareness and training policy and associated security *and privacy* awareness and training controls;

(vi) the organization disseminates documented security *and privacy* awareness and training procedures to *applicable personnel* within the organization having associated security *and privacy* awareness and training roles and responsibilities;

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

#### Assessment Methods And Objects

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

#### AT-2 – Security Awareness *Training* (Low)

*Assurance - PI*

#### Control

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

- a. As part of initial training for new users prior to accessing any system's information;
- b. When required by system changes; and
- c. Within every three hundred sixty-five (365) days thereafter.

#### *Implementation Standard(s)*

1. An information security and privacy education and awareness training program is developed and implemented for all employees and individuals working on behalf of CMS involved in managing, using, and/or operating information systems.
2. Privacy awareness training is provided before granting access to systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors, to explain the importance and responsibility in safeguarding PII and ensuring privacy, as established in Federal legislation and OMB guidance.

#### Guidance

*Organizations determine* the appropriate content of security *and privacy* awareness training, and security *and privacy* awareness techniques based on the specific *organizational* requirements *and* the information systems to which personnel have authorized

<p>access. The content includes a basic understanding of the need for information security and user actions to maintain security and <i>privacy</i>, and to respond to suspected security <i>and privacy</i> incidents. The content also addresses awareness of the need for operations security <i>and privacy</i> as it relates to CMS' information security program. Security <i>and privacy</i> awareness techniques can include, for example, displaying posters, offering supplies inscribed with security <i>and privacy</i> reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security <i>and privacy</i> awareness events.</p>	
<p><b>Reference(s):</b> <i>Executive Order: 13587</i>; FISCAM: <i>AS-1</i>, SM-4; HIPAA: 164.308(a)(5)(i), <i>164.308(a)(5)(ii)(A)</i>, <i>164.308(a)(5)(ii)(B)</i>; IRS-1075: 6.2#1.1-2, <i>9.4#1.2</i>; <i>NIST SP: 800-50</i></p>	<p><b>Related Controls Requirement(s):</b> <i>AT-3, AT-4, PL-4</i></p>
<p><b>ASSESSMENT PROCEDURE: AT-2.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;</li> <li>(ii) the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least <i>every three hundred sixty-five (365) days</i>;</li> <li>(iii) the organization provides refresher security awareness training in accordance with the organization-defined frequency.</li> <li>(iv) <i>the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> Security <i>and privacy</i> awareness and training policy; procedures addressing security <i>and privacy</i> awareness training implementation; appropriate codes of federal regulations; security <i>and privacy</i> awareness training curriculum; security <i>and privacy</i> awareness training materials; security plan; training records; other relevant documents or records.</p>	
<p><b>AT-3 – <i>Role-Based Security Training</i> (Low)</b></p>	
<p><b>Control</b></p> <p>The organization provides role-based security training <i>to personnel with assigned security roles and responsibilities</i>:</p> <ul style="list-style-type: none"> <li><i>a.</i> Before authorizing access to the <i>information</i> system or performing assigned duties;</li> <li><i>b.</i> When required by <i>information</i> system changes; and</li> <li><i>c.</i> Within every three hundred sixty-five (365) days thereafter.</li> </ul> <p><b>Implementation Standard(s)</b></p> <ol style="list-style-type: none"> <li>1. Require personnel with significant information security roles and responsibilities to undergo appropriate information system</li> </ol>	

security training prior to authorizing access to networks, systems, and/or applications; when required by *significant information system or system environment* changes; *when an employee enters a new position that requires additional role-specific training*; and refresher training within every three hundred sixty-five (365) days thereafter.

*2. (For CSP only) For service providers, the organization provides refresher training a least every three (3) years thereafter.*

#### Guidance

*Organizations determine* the appropriate content of security training based on *the* assigned roles and responsibilities *of individuals* and the specific *security* requirements of CMS and the information systems to which personnel have authorized access. In addition, *organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for* their assigned duties. *Comprehensive role-based* training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. *Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of CMS' information security programs. Role-based security training also applies to contractors providing services to federal agencies.*

**Reference(s):** FISCAM: AS-1, SM-4; *HIPAA: 164.308(a)(5)(i); IRS-1075: 9.3#2.2, 9.4#1.3; NIST SP: 800-16, 800-50*

**Related Controls Requirement(s):** *AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16*

#### ASSESSMENT PROCEDURE: AT-3.1

##### Assessment Objective

Determine if:

- (i) the organization provides role-based security- training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties, and when required by information system changes;*
- (ii) the organization provides role-based security-related refresher training within every three hundred sixty-five (365) days thereafter.*
- (iii) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

##### Assessment Methods And Objects

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

**AT-4 – Security Training Records (Low)**

**Assurance - P3**

**Control**

The organization:

- a. Documents and monitors individual information system security *and privacy* training activities including basic security *and privacy* awareness training and specific information system security *and privacy* training; and
- b. Retains individual training records for *a minimum of five (5) years*.

**Implementation Standard(s)**

1. *(For CSP only) For service providers, the organization retains individual training records for at least three (3) years.*

**Guidance**

Procedures and training implementation should:

- (a) Identify employees with significant information security *and privacy* 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 *and privacy* awareness materials at least *every 365 days*.

Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.

- 2) Executives must receive training in information security *and privacy* basics and policy level training in security *and privacy* planning and management.

- 3) Program and functional managers must receive training in information security *and privacy* basics; management and implementation level training in security *and privacy* planning and system/application security *and privacy* management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.

- 4) Chief Information Officers (CIOs), *information* security *and privacy* program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security *and privacy* officers) must receive training in information security *and privacy* basics and broad training in security *and privacy* planning, system and application security *and privacy* management, system/application life cycle management, risk management, and contingency planning.

- 5) IT function management and operations personnel must receive training in information security *and privacy* basics; management and implementation level training in security *and privacy* planning and system/application security *and privacy* management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.

- (b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on *information* security awareness and training to all new employees before allowing them access to the systems.

- (c) Provide information systems security *and privacy* refresher training for employees as frequently as determined necessary,

based on the sensitivity of the information that the employees use or process.

(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.

*Documentation for specialized training may be maintained by individual supervisors at the option of the organization.*

**Reference(s):** FISCAM: AS-1, SM-4; *HIPAA: 164.308(a)(5)(i)*; IRS-1075: 6.2#1.3

**Related Controls Requirement(s):** *AT-2, AT-3, PM-14*

#### **ASSESSMENT PROCEDURE: AT-4.1**

##### **Assessment Objective**

Determine if:

- (i) the organization documents and monitors individual information system security **and privacy** training activities including basic security **and privacy** awareness training and specific information system security **and privacy** training;*
- (ii) the organization retains individual training records in accordance with the organization-defined time period.*
- (iii) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

##### **Assessment Methods And Objects**

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



### 3.0 AUDIT AND ACCOUNTABILITY (AU)

*Error! Reference source not found.*

AU-1 – Audit and Accountability Policy and Procedures (Low)	Assurance - P1
<p><b>Control</b></p> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. Audit and accountability policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. Audit and accountability procedures within every three hundred sixty-five (365) days.</i></li> </ol>	
<p><b>Guidance</b></p> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>AU</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing policy and procedures</i>.</p>	
<p><b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; <i>HIPAA: 164.312(b); IRS-1075: 9.3#1; NIST SP: 800-12, 800-100</i></p>	<p><b>Related Controls Requirement(s):</b> <i>PM-9</i></p>
<p><b>ASSESSMENT PROCEDURE: AU-1.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ol style="list-style-type: none"> <li>the organization develops and documents audit and accountability policy;</li> <li>the organization audit and accountability policy addresses: <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> </ul> </li> </ol>	



- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented audit and accountability policy to *applicable personnel* within the organization having associated audit and accountability roles and responsibilities;

(iv) the organization develops and formally documents audit and accountability procedures;

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

(vi) the organization disseminates documented audit and accountability procedures to *applicable personnel* within the organization having associated audit and accountability roles and responsibilities.

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

#### Assessment Methods And Objects

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

#### AU-2 – Audit Events (Low)

*PI*

#### Control

The organization:

- a. Determines, based on a risk assessment and CMS mission/business needs, that the information system *is* capable of auditing the events specified in Implementation *Standard 1*;
- b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
- c. *Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and*
- d. Determines which events *specified in Implementation Standard 2* require auditing on a continuous basis *in* response to specific situations.

#### Implementation Standard(s)

1. *List of auditable* events:
  - (a) *Server alerts and error messages;*
  - (b) *User log-on and log-off (successful or unsuccessful);*
  - (c) *All system administration* activities;

- (d) Modification of privileges and access;*
- (e) Start up and shut down;*
- (f) Application modifications;*
- (g) Application alerts and error messages;*
- (h) Configuration changes; and*
- (i) Account creation, modification, or deletion; and*
- (j) File creation and deletion.*
- 2. Subset of Implementation Standard 1 auditable events:*
  - (a) User log-on and log-off (successful or unsuccessful);*
  - (b) All system administration activities;*
  - (c) Modification of privileges and access; and*
  - (d) Account creation, modification, or deletion.*
- 3. Verify that proper logging is enabled in order to audit administrator activities.*
- 5. (For CSP only) For service providers, this Standard replaces the above Control and Standards. The organization:*
  - a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events; and for Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes; and*
  - b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;*
  - c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and*
  - d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: organization-defined subset of the auditable events to be audited continually.*
- 6. (For CSP only) For service providers, the organization defines the subset of auditable events from AU-2a to be audited. The events to be audited are approved and accepted by Joint Authorization Board (JAB).*

#### **Guidance**

*An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying*

that subset of auditable events that are audited at a given point in time. For example, *organizations* may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the *potential burden on system performance*. *Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards.* Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the *appropriate* level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. *Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures.*

**Reference(s):** FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 9.3#2.1; *NIST SP: 800-92; Web: [csrc.nist.gov/pcig/cig.html](http://csrc.nist.gov/pcig/cig.html)*

**Related Controls Requirement(s):** *AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, SI-4*

#### **ASSESSMENT PROCEDURE: AU-2.1**

##### **Assessment Objective**

Determine if:

- (i)* the organization determines, based on a risk assessment and CMS mission/business needs, that the information system *is* capable of auditing the list of auditable events specified in the Implementation Standards;
- (ii)* the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events;
- (iii)* the organization defines in the security plan, explicitly or by reference, information system auditable events;
- (iv)* the organization *determines* the auditable events defined in *Implementation Std.2* to be audited within the information system, and the frequency of (or situation requiring) auditing for each identified event.
- (v)* the organization *provides a rationale for why* the auditable events *are deemed* to be *adequate to support after-the-fact investigations of security incidents*
- (vi)* the organization meets all the requirements specified in the applicable Implementation Standard(s).

##### **Assessment Methods And Objects**

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

<b>AU-3 – Content of Audit Records (Low)</b>		<b>PI</b>
<b>Control</b> <p>The information system <i>generates</i> audit records <i>containing</i> information <i>that establishes</i> what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any <i>individuals or subjects</i> associated with the event.</p>		
<b>Guidance</b> <p>Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. <i>Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).</i></p>		
<b>Reference(s):</b> FISCAM: AC-5, AS-2; <i>HIPAA: 164.312(b); IRS-1075: 9.3#3</i>		<b>Related Controls Requirement(s):</b> <i>AU-2, AU-8, AU-12, SI-11</i>
<b>ASSESSMENT PROCEDURE: AU-3.1</b>		
<b>Assessment Objective</b> <p>Determine if the information system <i>generates</i> audit records <i>containing</i> information <i>that establishes</i>:</p> <ul style="list-style-type: none"> <li>- what type of event occurred;</li> <li>- when the event occurred;</li> <li>- where the event occurred;</li> <li>- the source of the event;</li> <li>- the outcome of the event;</li> <li>- the identity of any <i>individuals or subjects</i> associated with the event.</li> </ul>		
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> 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.</p>		
<b>AU-4 – Audit Storage Capacity (Low)</b>		<b>PI</b>
<b>Control</b> <p>The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.</p>		
<b>Guidance</b> <p>The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit</p>		

storage capacity. *Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.*

**Reference(s):** FISCAM: AC-5, *AS-2*; *HIPAA: 164.312(b)*; IRS-1075: 9.3#5

**Related Controls Requirement(s):** AU-2, AU-5, AU-6, AU-7, *AU-11*, SI-4

#### ASSESSMENT PROCEDURE: AU-4.1

##### Assessment Objective

Determine if:

- (i)* the organization allocates 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 (Low)

*PI*

##### Control

The information system:

- a. Alerts designated organizational officials in the event of an audit processing failure; and
- b. Takes the following additional actions in response to an audit failure or audit storage capacity issue:
  - Shutdown the information system,
  - Stop generating audit records, or
  - Overwrite the oldest records, in the case that storage media is unavailable.

##### *Implementation Standard(s)*

*1. (For CSP only) For service providers, the information system takes the following actions in the event of an audit processing failure: overwrite oldest audit records.*

##### Guidance

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. *Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of*

<i>organizations (i.e., all audit data storage repositories combined), or both.</i>	
<b>Reference(s):</b> FISCAM: AC-5, <i>AS-2</i>	<b>Related Controls Requirement(s):</b> AU-4, <i>SI-12</i>
<b>ASSESSMENT PROCEDURE: AU-5.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li><i>(i) the organization defines designated organizational officials to be alerted in the event of an audit processing failure;</i></li> <li><i>(ii) the organization defines in the security plan, explicitly or by reference, personnel to be notified in case of an audit processing failure;</i></li> <li><i>(iii) the organization defines additional actions to be taken in the event of an audit processing failure;</i></li> <li><i>(iv) the information system takes the additional organization-defined actions in the event of an audit processing failure.</i></li> <li><i>(v) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.</p>	
<b>AU-6 – Audit Review, Analysis, and Reporting (Low)</b>	
<i>Assurance - PI</i>	
<p><b>Control</b></p> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity; and</li> <li><i>b. Reports findings to designated organizational officials.</i></li> </ul> <p><b>Implementation Standard(s)</b></p> <ol style="list-style-type: none"> <li>1. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment.</li> <li>2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment.</li> <li>3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.</li> </ol>	

4. Use automated utilities to review audit records at least once *weekly* for unusual, unexpected, or suspicious behavior.
5. Inspect administrator groups on demand but no less than once every thirty (30) days to ensure unauthorized administrator accounts have not been created.
8. *(For CSP only) For service providers, the organization reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials.*

**Guidance**

*Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority.*

**Reference(s):** FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 9.3#6

**Related Controls Requirement(s):** AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-4, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7

**ASSESSMENT PROCEDURE: AU-6.1**

**Assessment Objective**

Determine if:

- (i)* the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency;
- (ii)* the organization report to designated organizational officials.
- (iii)* the organization meets all the requirements specified in the applicable Implementation Standard(s).

**Assessment Methods And Objects**

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

<b>AU-8 – Time Stamps (Low)</b>		<b>P1</b>
<b>Control</b> <p>The information system:</p> <ul style="list-style-type: none"> <li>a. Uses internal system clocks to generate time stamps for audit records; <i>and</i></li> <li>b. <i>Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and is accurate to within thirty (30) seconds.</i></li> </ul>		
<b>Guidance</b> <p>Time stamps generated by the information system include date and time. <i>Time is commonly</i> expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. <i>Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.</i></p>		
<b>Reference(s):</b> FISCAM: AC-5, AS-2		<b>Related Controls Requirement(s):</b> AU-3, AU-12
<b>ASSESSMENT PROCEDURE: AU-8.1</b>		
<b>Assessment Objective</b> <p>Determine if the information system uses internal system clocks to generate time stamps for audit records <i>and records time stamps for audit records that can be mapped to UTC or GMT and is accurate to within thirty (30) seconds.</i></p>		
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> 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.</p>		
<b>AU-9 – Protection of Audit Information (Low)</b>		<b>P1</b>
<b>Control</b> <p>The information system protects audit information and audit tools from unauthorized access, modification, and deletion.</p>		
<b>Guidance</b> <p>Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. <i>This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.</i></p>		



Reference(s): FISCAM: AC-5, <i>AS-2</i>	Related Controls Requirement(s): <i>AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6</i>
<b>ASSESSMENT PROCEDURE: AU-9.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if the information system protects audit information and audit tools from unauthorized:</p> <ul style="list-style-type: none"> <li>- access;</li> <li>- modification;</li> <li>- deletion.</li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> 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.</p>	
<b>AU-11 – Audit Record Retention (Low)</b>	
<p><b>Control</b></p> <p>The organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and CMS information retention requirements.</p> <p><b>Implementation Standard(s)</b></p> <p><i>4. (For CSP only) For service providers, the organization retains audit records on-line for at least ninety (90) days and further preserves audit records off-line for a period that is in accordance with NARA requirements.</i></p>	
<p><b>Guidance</b></p> <p><i>Organizations retain</i> audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. <i>Organizations develop standard categories</i> of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.</p>	
Reference(s): FISCAM: AC-5, <i>AS-2</i> ; <i>IRS-1075: 3.1#1, 9.3#7</i>	Related Controls Requirement(s): <i>AU-4, AU-5, AU-9, MP-6</i>
<b>ASSESSMENT PROCEDURE: AU-11.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p>	

- (i) the retention period for audit records is consistent with the records retention policy;
- (ii) the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
- (vi) *(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

#### Assessment Methods And Objects

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

#### AU-12 – Audit Generation (Low)

*P1*

#### Control

The information system:

a. Provides audit record generation capability for the following *auditable* events *defined* in *AU-2a*:

- All successful and unsuccessful authorization attempts.
- All changes to logical access control authorities (e.g., rights, permissions).
- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
- The audit trail shall capture the enabling or disabling of audit report generation services.
- The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the *information* system; and

c. Generates audit records for the list of events defined in *AU-2d* with the content defined in *AU-3*.

#### *Implementation Standard(s)*

*1. (For CSP only) For service providers, the information system provides audit record generation capability for the list of auditable events defined in AU-2 at all information system components where audit capability is deployed.*

#### Guidance

Audit records can be generated from *many different* information system *components*. The list of audited events is the set of events for which audits are to be generated. *These* events *are* typically a subset of all events for which the *information* system is capable of generating audit records.

#### Reference(s):

**Related Controls Requirement(s):** *AC-3, AU-2, AU-3, AU-6, AU-7*

**ASSESSMENT PROCEDURE: AU-12.1**

**Assessment Objective**

Determine if:

- (i) the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2a;
- (ii) the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2;
- (iii) the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the *information* system;
- (iv) the information system generates audit records for the list of events defined in AU-2d with the content as defined in AU-3.
- (v) *(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

**Assessment Methods And Objects**

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

## 4.0 SECURITY ASSESSMENT AND AUTHORIZATION (CA)

*Error! Reference source not found.*

CA-1 – Security Assessment and Authorization Policies and Procedures (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li>1. A security assessment and authorization policy that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and</li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li>1. Security assessment and authorization policy within every three hundred sixty-five (365) days; and</li> <li>2. Security assessment and authorization procedures within every three hundred sixty-five (365) days.</li> </ol>		
<b>Guidance</b> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>CA</i> family. <i>Policy</i> and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. <i>The policy</i> can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations</i>. The procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing policy and procedures</i>.</p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 9.5#1; NIST SP: 800-12, 800-37, 800-53A, 800-100		<b>Related Controls Requirement(s):</b> PM-9
<b>ASSESSMENT PROCEDURE: CA-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <p><i>(i)</i> the organization develops and documents security assessment and authorization policy;</p> <p><i>(ii)</i> the organization security assessment and authorization policy addresses:</p> <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> </ul>		

- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented security assessment and authorization policy to *applicable personnel* within the organization having associated security assessment and authorization roles and responsibilities;

(iv) the organization develops and documents security assessment and authorization procedures;

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

(vi) the organization disseminates documented security assessment and authorization procedures to *applicable personnel* within the organization having associated security assessment and authorization roles and responsibilities;

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

#### Assessment Methods And Objects

**Examine:** Security assessment and authorization policies and procedures; other relevant documents or records.

#### CA-2 – Security Assessments (Low)

*Assurance - P2*

#### Control

The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:

1. Security controls and control enhancements under assessment;
2. Assessment procedures to be used to determine security control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system *and its environment of operation* within every three hundred sixty-five (365) days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting *established* security requirements;

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

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

#### Implementation Standard(s)

1. *An independent* security assessment of all security controls must be conducted prior to issuing the authority to operate for all newly implemented, *or significantly changed*, systems.
2. The annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period.
3. The Business Owner notifies the CMS CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO).

## Guidance

*Organizations assess* security controls in *organizational* information system *and the environments in which those systems operate* as part of: (i) *initial and ongoing* security *authorizations*; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle *activities*. *Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from NIST 800-53 Appendix F (main catalog) and NIST 800-53 Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document* assessment results in sufficient detail as deemed necessary by CMS, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for *assessing security controls* at least *annually does not require* additional assessment *activities* to those *activities* already in place in *organizational* security authorization *processes*. *Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.*

To satisfy annual assessment requirements, organizations can *use* assessment results from the following sources, including but not limited to: (i) *initial or ongoing* information system *authorizations*; (ii) continuous monitoring; or (iii) system development life cycle *activities*. *Organizations ensure* that *security assessment* results are current, relevant to the determination of security control effectiveness; *and obtained with the appropriate level of assessor independence*. Existing security control assessment results *can be* reused to the extent that *the results* are still valid and *can also be* supplemented with additional assessments as needed. Subsequent to initial *authorizations* and in accordance with OMB policy, *organizations assess* security controls during continuous monitoring. *Organizations establish* the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical to

protecting CMS operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the FISMA annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. *Vulnerability Alerts provide useful examples of vulnerability mitigation procedures.* External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control.

**Reference(s):** *Executive Order: 13587; FIPS Pub: 199; FISCAM: AS-1, SM-5; HIPAA: 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 6.3#4, 6.3.5#1, 9.5#2; NIST SP: 800-37, 800-39, 800-53A, 800-115, 800-137*

**Related Controls Requirement(s):** CA-5, CA-6, CA-7, *PM-9, RA-5*, SA-11, *SA-12*, SI-4

#### ASSESSMENT PROCEDURE: CA-2.1

##### Assessment Objective

Determine if:

- (i) the organization develops a security assessment plan for the information system;
- (ii) the security assessment plan describes the scope of the assessment including:
  - security controls and control enhancements under assessment;
  - assessment procedures to be used to determine security control effectiveness;
  - assessment environment, assessment team, and assessment roles and responsibilities.
- (iii) the organization meets all the requirements specified in the applicable Implementation Standard(s).

##### Assessment Methods And Objects

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

#### ASSESSMENT PROCEDURE: CA-2.2

##### Assessment Objective

Determine if:

- (i) the organization assesses the security controls in the information system within every three hundred sixty-five (365) days in accordance with the CMS IS ARS Including CMSR Standard, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting *established* security requirements;
- (ii) the organization provides the results of the security control assessment within every 365 days, in writing, to the Business Owner;
- (iii) the Business Owner reviews the assessment documentation and updates system security documentation where necessary to

reflect any changes to the system;

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

### Assessment Methods And Objects

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

### CA-2(1) - Independent Assessors – Enhancement (Low)

Assurance - P2

#### Control

*(For CSP only) The organization employs assessors or assessment teams with FedRAMP defined level of independence to conduct security control assessments.*

#### **Implementation Standard(s)**

*1. (For CSP only) For service providers, the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.*

#### Guidance

*(For CSP only) Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent*



*teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.*

**Reference(s):**

**Related Controls Requirement(s):**

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

**Assessment Objective**

*Determine if:*

- (i) (For CSP only) the organization employs assessors or assessment teams to conduct security control assessments.*
- (ii) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

**Assessment Methods And Objects**

**Examine:** *(For CSP only) Security assessment and authorization policy; procedures addressing security assessments; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.*

**Interview:** *(For CSP only) Organizational personnel with security assessment responsibilities.*

**CA-3 – System Interconnections (Low)**

**Assurance - P1**

**Control**

*The organization:*

- a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;*
- b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and*
- c. Reviews and updates the Interconnection Security Agreements on an ongoing basis verifying enforcement of security requirements.*

**Implementation Standard(s)**

1. Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the system that is connected to the remote location.
2. *The Interconnection Security Agreement or data sharing agreement is updated following significant changes to the system, organizations, or the nature of the electronic sharing of information that could impact the validity of the agreement.*

**Guidance**

This control applies to dedicated connections between information systems (*i.e., system interconnections*) and does not apply to

transitory, user-controlled connections such as email and website browsing. *Organizations* carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within *organizations* and external to *organizations*. *The CMS authorizing official determines* the risk associated with *information system connections* and the appropriate controls employed. If interconnecting systems have the same *CMS Business Owner*, an Interconnection Security Agreement is not required. *Instead*, interface characteristics between the interconnecting information systems *can be* described in the security plans for *their* respective systems. If the interconnecting systems have different *CMS Business Owners* but the *Business Owners* are in the same organization, the *organizations determine* whether *either a Memorandum of Understanding (MOU) and/or Service Level Agreement (SLA)* is required. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into formal contracts, especially if the interconnection is to be established between CMS and a nonfederal (private sector) organization. Risk considerations also include information systems sharing the same networks. *For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls.*

**Reference(s):** *FIPS Pub: 199; FISCAM: AC-1, AS-2; HIPAA: 164.308(b)(1), 164.308(b)(4), 164.314(a)(2)(ii); HSPD 7: F(19); NIST SP: 800-47*

**Related Controls Requirement(s):** *AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4*

#### **ASSESSMENT PROCEDURE: CA-3.1**

##### **Assessment Objective**

Determine if:

- (i)* the organization identifies connections to external information systems;
- (ii)* the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;
- (iii)* the organization documents, for each *inter*connection, the interface characteristics, security requirements, and the nature of the information communicated;
- (iv)* the organization *reviews and updates* the *Interconnection Security Agreement* on an ongoing basis to verify enforcement of security requirements.
- (v)* the organization meets all the requirements specified in the applicable Implementation Standard(s).

##### **Assessment Methods And Objects**

**Examine:** Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records.

<b>CA-5 – Plan of Action and Milestones (Low)</b>		<b>Assurance - P3</b>
<b>Control</b> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Develops and submits a plan of action and milestones for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., SCA, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and</i></li> <li><i>b. Updates and submits existing plan of action and milestones monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.</i></li> </ul> <p><b>Implementation Standard(s)</b></p> <ul style="list-style-type: none"> <li><i>1. (For CSP only) For service providers, the organization updates existing plan of action and milestones at least quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.</i></li> </ul>		
<b>Guidance</b> <p><i>Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB.</i></p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-6; HIPAA: 164.308(a)(2), 164.308(a)(8); HSPD 7: F(19), G(24); IRS-1075: 6.4#1, 9.5#4; NIST SP: 800-37; OMB: M-02-01		<b>Related Controls Requirement(s):</b> CA-2, CA-7, CM-4, PM-4
<b>ASSESSMENT PROCEDURE: CA-5.1</b>		
<b>Assessment Objective</b> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization develops a plan of action and milestones for the information system within thirty (30) days of the final results for every internal/external audit/review or test;</i></li> <li><i>(ii) the plan of action and milestones documents the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system;</i></li> <li><i>(iii) the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates;</i></li> <li><i>(iv) the organization updates and submits existing plan of action and milestones monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.</i></li> <li><i>(v) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul>		
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan;</p>		

security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.

**CA-5(1) - Automation Support for Accuracy/Currency – Enhancement (Low)**

**Assurance - P3**

**Control**

The organization employs automated mechanisms to help ensure that the *plan of action and milestones* for the information system is accurate, up to date, and readily available.

**Reference(s):**

**Related Controls Requirement(s):**

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

**Assessment Objective**

Determine if the organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is:

- accurate;
- up to date;
- readily available.

**Assessment Methods And Objects**

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

**CA-6 – Security Authorization (Low)**

**Assurance - P3**

**Control**

*The organization:*

*a. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and*

*b. Updates the security authorization:*

- *Within every three (3) years;*
- *When significant changes are made to the system;*
- *When changes in requirements result in the need to process data of a higher sensitivity;*
- *When changes occur to authorizing legislation or federal requirements;*
- *After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization;*
- and*
- *Prior to expiration of a previous security authorization.*

**Guidance**

*Security authorizations are official management decisions, conveyed through authorization decision documents, by the CMS CIO or his/her designated representative (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to CMS operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Explicit authorization to operate the information system is provided by the CMS CIO or his/her designated representative prior to a system being placed into operations. Through the security authorization process, the CMS CIO is accountable for security risks associated with the operation and use of CMS information system.*

*OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing the CMS CIO and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, the CMS CIO uses results of the continuous monitoring processes to the maximum extent possible as the basis for rendering a reauthorization decisions.*

*(For CSP only) Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would require a reauthorization of the information system. The types of changes are approved and accepted by the Joint Authorization Board (JAB).*

**Reference(s):** FISCAM: AS-1, SM-2; HIPAA: 164.308(a)(2), 164.308(a)(8); HSPD 7: F(19); NIST SP: 800-37, 800-137; OMB: Circular A-130, M-11-33

**Related Controls Requirement(s):** CA-2, CA-7, PM-9, PM-10

**ASSESSMENT PROCEDURE: CA-6.1**

**Assessment Objective**

*Determine if:*

- (i) the organization defines in the security plan, explicitly or by reference, the frequency of authorization updates, not to exceed three years;*
- (ii) the organization ensures that the authorizing official authorizes the information system for processing before commencing operations;*
- (iii) the organization updates the security authorization:*
  - within every three (3) years;*
  - when significant changes are made to the system;*
  - when changes in requirements result in the need to process data of a higher sensitivity;*
  - when changes occur to authorizing legislation or federal requirements;*

- after the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
- prior to expiration of a previous security authorization;
- (iv) a senior organizational official signs and approves the security authorization package.

#### **Assessment Methods And Objects**

**Examine:** Security assessment and authorization policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.

#### **CA-7 – Continuous Monitoring (Low)**

**Assurance - P3**

#### **Control**

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

- a. Establishment of defined metrics (defined in the applicable security plan) to be monitored;
- b. Establishment of defined frequencies (defined in the applicable security plan) for monitoring and defined frequencies (defined in the applicable security plan) for assessments supporting such monitoring;
- c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
- e. Correlation and analysis of security-related information generated by assessments and monitoring;
- f. Response actions to address results of the analysis of security-related information; and
- g. Reporting the security status of organization and the information system to appropriate organizational officials monthly.

#### **Guidance**

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide

<i>information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems.</i>	
<b>Reference(s):</b> FISCAM: <i>AS-1</i> , SM-5; <i>HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(8);</i> HSPD 7: F(19); <i>NIST SP: 800-37, 800-39, 800-53A, 800-115, 800-137; OMB: M-11-33</i>	<b>Related Controls Requirement(s):</b> CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4
<b>ASSESSMENT PROCEDURE: CA-7.1</b>	
<b>Assessment Objective</b> Determine if: <i>(i) the organization develops a continuous monitoring strategy and program;</i> <i>(ii) the organization defines organizational officials to whom the security state of the information system should be reported;</i> <i>(iii) the organization implements a continuous monitoring program that includes:</i> - a configuration management process for the information system and its constituent components; - a determination of the security impact of changes to the information system and environment of operation; - ongoing security control assessments in accordance with the organizational continuous monitoring strategy; - reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.	
<b>Assessment Methods And Objects</b> <b>Examine:</b> Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records.	
<b>CA-7(2) - Types of Assessments – Enhancement (Low)</b>	
<b>Control</b>	
<i>[Withdrawn: Incorporated into CA-2(2)].</i>	
<b>CA-9 – Internal System Connections (Low)</b>	
<b>Control</b>	
The organization: <i>a. Authorizes connections of defined internal information system components or classes of components (defined in the applicable security plan) to the information system; and</i> <i>b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information</i>	

<i>communicated.</i>	
<b>Guidance</b> <i>This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.</i>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s):</b> AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4
<b>ASSESSMENT PROCEDURE: CA-9.1</b>	
<b>Assessment Objective</b> Determine if: <i>(i) the organization authorizes connections of defined internal information system components or classes of components to the information system;</i> <i>(ii) the organization documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.</i>	
<b>Assessment Methods And Objects</b> <b>Examine:</b> Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records. <b>Interview:</b> Organizational personnel with <i>component connection authorization</i> responsibilities.	



## 5.0 CONFIGURATION MANAGEMENT (CM)

*Error! Reference source not found.*

CM-1 – Configuration Management Policy and Procedures (Low)	Assurance - P1
<p><b>Control</b></p> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. Configuration management policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. Configuration management procedures within every three hundred sixty-five (365) days.</i></li> </ol> <p><b>Implementation Standard(s)</b></p> <ol style="list-style-type: none"> <li><i>1. The configuration management process and procedure is documented to define configuration items at the system and component level (e.g., hardware, software, workstation); monitor configurations; and track and approve changes prior to implementation, including, but not limited to, flaw remediation, security patches, and emergency changes (e.g., unscheduled changes such as mitigating newly discovered security vulnerabilities, system crashes, replacement of critical hardware components).</i></li> </ol>	
<p><b>Guidance</b></p> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>CM</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing policy and procedures</i>.</p>	
<p><b>Reference(s):</b> FISCAM: AS-1, <i>AS-3</i>, CM-1, SM-1, SM-3; IRS-1075: 9.6#1; <i>NIST SP: 800-12, 800-100</i></p>	<p><b>Related Controls Requirement(s):</b> <i>PM-9</i></p>

<b>ASSESSMENT PROCEDURE: CM-1.1</b>	
<b>Assessment Objective</b> Determine if: <i>(i)</i> the organization develops and formally documents configuration management policy; <i>(ii)</i> the organization configuration management policy addresses: - purpose; - scope; - roles and responsibilities; - management commitment; - coordination among organizational entities; - compliance; <i>(iii)</i> the organization disseminates documented configuration management policy to <i>applicable personnel</i> within the organization having associated configuration management roles and responsibilities; <i>(iv)</i> the organization develops and documents configuration management procedures; <i>(v)</i> the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls; <i>(vi)</i> the organization disseminates documented configuration management procedures to <i>applicable personnel</i> within the organization having associated configuration management roles and responsibilities; <i>(vii)</i> the organization reviews <i>and</i> updates the configuration management policy and procedures within every three hundred sixty-five (365) days. <i>(viii) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i>	
<b>Assessment Methods And Objects</b> <b>Examine:</b> Configuration management policy and procedures; other relevant documents or records.	
<b>CM-2 – Baseline Configuration (Low)</b>	<b>Assurance - P1</b>
<b>Control</b> The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	
<b>Guidance</b> This control establishes baseline configurations for information systems and <i>system</i> components including communications and connectivity-related aspects of <i>systems</i> . <i>Baseline configurations are documented, formally reviewed and agreed-upon sets of</i>	

<p><i>specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.</i></p>	
<p><b>Reference(s):</b> <i>FISCAM: AS-3, CM-2; NIST SP: 800-128</i></p>	<p><b>Related Controls Requirement(s):</b> <i>CM-3, CM-6, CM-8, CM-9, PM-5, PM-7, SA-10</i></p>
<p><b>ASSESSMENT PROCEDURE: CM-2.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li><i>(i) the organization develops and documents a baseline configuration of the information system;</i></li> <li><i>(ii) the organization maintains, under configuration control, a current baseline configuration of the information system.</i></li> <li><i>(iii) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.</p>	
<p><b>CM-4 – Security Impact Analysis (Low)</b> <span style="float: right;"><i>Assurance - P2</i></span></p>	
<p><b>Control</b></p> <p>The organization analyzes changes to the information system to determine potential security <i>and privacy</i> impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.</p>	
<p><b>Guidance</b></p> <p>Organizational personnel with information security responsibilities (<i>e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers</i>) <i>conduct security impact analyses</i>. Individuals conducting security impact analyses <i>possess</i> the <i>necessary</i> skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security <i>control requirements</i> and <i>reviewing system design documentation to understand control implementation and how specific</i> changes might affect the controls. Security impact analyses may also include <i>assessments</i> of risk</p>	

to *better* understand the impact of the changes and to determine if additional security controls are required. Security impact *analyses are* scaled in accordance with the security categories of the information systems.

**Reference(s):** FISCAM: AS-3, CM-4; *NIST SP: 800-128*

**Related Controls Requirement(s):** CA-2, CA-7, CM-3, *CM-9, SA-4, SA-5, SA-10, SI-2*

#### **ASSESSMENT PROCEDURE: CM-4.1**

##### **Assessment Objective**

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

##### **Assessment Methods And Objects**

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

#### **CM-6 – Configuration Settings (Low)**

**P1**

##### **Control**

*The organization:*

- a. Establishes and documents configuration settings for information technology products employed within the information system using the latest security configuration baselines established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 (refer to Implementation Standard 1 for specifics) that reflect the most restrictive mode consistent with operational requirements;*
- b. Implements the configuration settings;*
- c. Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements; and*
- d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.*

##### **Implementation Standard(s)**

- 1. (a) HHS-specific minimum security configurations shall be used for the following Operating System (OS) and Applications:*
  - HHS FDCC Windows XP Standard*
  - HHS FDCC Windows Vista Standard*
  - Blackberry Server*
  - Websense.*

*(b) For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is as follows:*

*(1) USGCB*

*(2) NIST National Checklist Program (NCP); Tier IV, then Tier III, Tier II, and Tier I, in descending order.*

*(3) Defense Information Systems Agency (DISA) STIGs*

*(4) National Security Agency (NSA) STIGs*

*(5) If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center for Internet Security [CIS]) checklists.*

*(6) In situations where no guidance exists, coordinate with CMS for guidance. CMS shall collaborate within CMS and the HHS Cybersecurity Program, and other OPDIVs through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to establish baselines and communicate industry and vendor best practices.*

*(7) All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented in an approved HHS waiver (available at [http://intranet.hhs.gov/it/cybersecurity/policies\\_by\\_document\\_type/index.html#Policy and Standard Waiver](http://intranet.hhs.gov/it/cybersecurity/policies_by_document_type/index.html#Policy%20and%20Standard%20Waiver)), with copies submitted to the Department.*

*2. (For CSP only) For service providers, the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using United States Government Configuration Baseline (USGCB) that reflect the most restrictive mode consistent with operational requirements.*

*3. (For CSP only) For service providers, the organization shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establish own configuration settings if USGCB is not available. Configuration settings are approved and accepted by the Joint Authorization Board (JAB).*

*4. (For CSP only) For service providers, the organization ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).*

### **Guidance**

*Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part*

*of the systems configuration baseline.*

*Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. (For CSP only) Information on the USGCB checklists can be found at: [http://usgcb.nist.gov/usgcb\\_faq.html#usgcbfaq\\_usgcbfdcc](http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc).*

**Reference(s):** FISCAM: AS-3, CM-2; IRS-1075: 9.6#1; NIST SP: 800-70, 800-128; OMB: M-07-11, M-07-18, M-08-22; Web: [checklists.nist.gov](http://checklists.nist.gov), [nsa.gov](http://nsa.gov), [nvd.nist.gov](http://nvd.nist.gov)

**Related Controls Requirement(s):** AC-19, CM-2, CM-3, CM-7, SI-4

#### **ASSESSMENT PROCEDURE: CM-6.1**

##### **Assessment Objective**

*Determine if:*

- (i) the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;*
- (ii) the organization establishes and documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;*
- (iii) the organization implements the security configuration settings;*
- (iv) the organization identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements;*
- (v) the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.*
- (vi) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

##### **Assessment Methods And Objects**

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

<b>CM-7 – Least Functionality (Low)</b>		<b>P1</b>
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Configures the information system to provide only essential capabilities; and</i></li> <li><i>b. Prohibits or restricts the use of high-risk system services, ports, network protocols, and capabilities (e.g., Telnet FTP, etc.) across network boundaries that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.</i></li> </ul> <p><b>Implementation Standard(s)</b></p> <ul style="list-style-type: none"> <li><i>1. (For CSP only) For service providers, this Standard replaces the above Control. The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: United States Government Configuration Baseline (USGCB)-defined list of prohibited or restricted functions, ports, protocols, and/or services.</i></li> <li><i>2. (For CSP only) For service providers, the organization shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. The list of prohibited or restricted functions, ports, protocols, and/or services are approved and accepted by the Joint Authorization Board (JAB).</i></li> </ul>		
<p><b>Guidance</b></p> <p><i>Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.</i></p> <p><i>(For CSP only) Information on the USGCB checklists can be found at: <a href="http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc">http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc</a>.</i></p>		
<p><b>Reference(s):</b> FISCAM: AC-3, AS-2; IRS-1075: 9.6#1</p>		<p><b>Related Controls Requirement(s):</b> AC-6, CM-2, RA-5, SA-5, SC-7</p>



**ASSESSMENT PROCEDURE: CM-7.1**

**Assessment Objective**

*Determine if:*

*(i) the organization defines for the information system prohibited or restricted:*

- functions;*
- ports;*
- protocols;*
- services;*

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

*(iii) the organization configures the information system to specifically prohibit or restrict the use of organization-defined:*

- functions;*
- ports;*
- protocols; and/or*
- services.*

*(iv) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

**Assessment Methods And Objects**

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

**CM-8 – Information System Component Inventory (Low)**

**Assurance - P1**

**Control**

*The organization:*

*a. Develops and documents an inventory of information system components that:*

- 1. Accurately reflects the current information system;*
- 2. Includes all components within the authorization boundary of the information system;*
- 3. Is at the level of granularity deemed necessary for tracking and reporting; and*
- 4. Includes:*
  - Unique identifier and/or serial number;*
  - Information system of which the component is a part;*
  - Type of information system component (e.g., server, desktop, application);*
  - Manufacturer/model information;*



- *Operating system type and version/service pack Level;*
- *Presence of virtual machines;*
- *Application software version/license information;*
- *Physical location (e.g., building/room number);*
- *Logical location (e.g., IP address, position with the IS architecture);*
- *Media access control (MAC) address;*
- *Ownership;*
- *Operational status;*
- *Primary and secondary administrators;*
- *Primary user; and*

*b. Reviews and updates the information system component inventory no less than annually, or per CM-8(1) and/or CM-8(2), as applicable.*

***Implementation Standard(s)***

- 1. All Government-owned equipment (i.e., servers, workstations, laptops, and other IT components) used to process, store, or transmit CMS information display an asset tag with a unique identifying asset number. IT components with an asset tag are tracked in an asset inventory database to include (at a minimum) name, location, asset identification, owner, and description of use.*
- 2. (For CSP only) For service providers, the organization develops, documents, and maintains an inventory of information system components that includes organization-defined information deemed necessary to achieve effective property accountability.*
- 3. (For CSP only) For service providers, the organization defines information deemed necessary to achieve effective property accountability. Property accountability information are approved and accepted by the Joint Authorization Board (JAB).*

***Guidance***

*Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.*

*(For CSP only) Information deemed necessary to achieve effective property accountability may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.*

<b>Reference(s):</b> FISCAM: AS-3, CM-2; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST SP: 800-128	<b>Related Controls Requirement(s):</b> CM-2, CM-6, PM-5
<b>ASSESSMENT PROCEDURE: CM-8.1</b>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization develops and documents an inventory of information system components that:</i> <ul style="list-style-type: none"> <li><i>- accurately reflects the current information system;</i></li> <li><i>- includes all components within the authorization boundary of the information system;</i></li> <li><i>- is at the level of granularity deemed necessary for tracking and reporting;</i></li> <li><i>- includes organization-defined information deemed necessary to achieve effective property accountability;</i></li> <li><i>- is available for review and audit by designated organizational officials.</i></li> </ul> </li> <li><i>(ii) the organization reviews and updates the information system component inventory no less than annually, or per CM-8(1) and/or CM-8(2), as applicable.</i></li> <li><i>(iii) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> Configuration management policy; configuration management plan; procedures addressing information system <i>component inventory</i>; security <i>plan</i>; information system <i>inventory</i> records; other relevant documents or records.</p>	
<b>CM-10 – Software Usage Restrictions (Low)</b>	
<p><b>Control</b></p> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. Uses software and associated documentation in accordance with contract agreements and copyright laws;</li> <li>b. <i>Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and</i></li> <li>c. <i>Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.</i></li> </ul>	
<p><b>Guidance</b></p> <p><i>Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.</i></p>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s):</b> AC-17, CM-8, SC-7

<b>ASSESSMENT PROCEDURE: CM-10.1</b>	
<b>Assessment Objective</b> Determine if: <i>(i) the organization uses software and associated documentation in accordance with contract agreements and copyright laws;</i> <i>(ii) the organization tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution;</i> <i>(iii) the organization controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.</i>	
<b>Assessment Methods And Objects</b> <b>Examine:</b> <i>Software use policy, contract agreements, site licenses, software installation policy and procedures, file sharing policy, security plan; other relevant documents or records.</i>	
<b>CM-11 – User-Installed Software (Low)</b>	
<b>Control</b>	
<i>The organization:</i> <i>a. Establishes organization-defined policies governing the installation of software by users;</i> <i>b. Enforces software installation policies through organization-defined methods; and</i> <i>c. Monitors policy compliance at organization-defined frequency.</i>	
<b>Guidance</b>	
<i>If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.</i>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s):</b> <i>AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4</i>

**ASSESSMENT PROCEDURE: CM-11.1**

**Assessment Objective**

*Determine if the organization:*

- establishes organization-defined policies governing the installation of software by users;*
- enforces software installation policies through organization-defined methods; and*
- monitors policy compliance at organization-defined frequency.*

**Assessment Methods And Objects**

**Examine:** *Software use policy, contract agreements, site licenses, software installation policy and procedures, file sharing policy, security plan; other relevant documents or records.*

## 6.0CONTINGENCY PLANNING (CP)

*Error! Reference source not found.*

<i>CP-1 – Contingency Planning Policy and Procedures (Low)</i>		<i>Assurance - P1</i>
<b>Control</b> <p><i>The organization:</i></p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. Contingency planning policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. Contingency planning procedures within every three hundred sixty-five (365) days.</i></li> </ol>		
<b>Guidance</b> <p><i>This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.</i></p>		
<b>Reference(s):</b> <i>FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(7)(i); IRS-1075: 9.7#2; NIST SP: 800-12, 800-34, 800-100</i>		<b>Related Controls Requirement(s):</b> <i>PM-9</i>
<b>ASSESSMENT PROCEDURE: CP-1.1</b>		
<b>Assessment Objective</b> <p><i>Determine if:</i></p> <ol style="list-style-type: none"> <li><i>the organization develops and documents contingency planning policy;</i></li> <li><i>the organization contingency planning policy addresses:</i> <ul style="list-style-type: none"> <li><i>- purpose;</i></li> <li><i>- scope;</i></li> </ul> </li> </ol>		

- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented contingency planning policy to applicable personnel within the organization having associated contingency planning roles and responsibilities;

(iv) the organization develops and documents contingency planning procedures;

(v) the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls;

(vi) the organization disseminates documented contingency planning procedures to applicable personnel within the organization having associated contingency planning roles and responsibilities;

(vii) the organization reviews and updates the contingency planning policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

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

#### CP-2 – Contingency Plan (Low)

PI

#### Control

The organization:

a. Develops a contingency plan for the information system in accordance with NIST SP 800-34 that:

1. Identifies essential CMS missions and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

6. Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the contingency plan to the Information System Security Officer, Business Owner, Contingency Plan Coordinator, and other stakeholders identified within the contingency plan;

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system within every three hundred sixty-five (365) days;

- e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;*
- f. Communicates contingency plan changes to key contingency personnel and organizational elements identified above; and*
- g. Protects the contingency plan from unauthorized disclosure and modification.*

**Implementation Standard(s)**

- 1. (For CSP only) For service providers, the organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to distribute the contingency plan to. The contingency list includes designated FedRAMP personnel.*
- 2. (For CSP only) For service providers, the organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to communicate any contingency plan changes to. The contingency list includes designated FedRAMP personnel.*

**Guidance**

Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business *functions*. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. *The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired.* Information system recovery objectives *reflect* applicable laws, Executive Orders, directives, policies, standards, regulations, *and guidelines*. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission *and/or* business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information *systems*. *Actions addressed* in contingency plans include, for example, *orderly/graceful* degradation, information system shutdown, *fallback* to a manual mode, alternate information flows, *and* operating in *modes* reserved for when *systems are* under attack. *By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.*

**Reference(s):** FISCAM: AS-5, CP-3; HIPAA: 164.308(a)(7)(ii)(*B*), 164.308(a)(7)(ii)(*C*), 164.308(a)(7)(ii)(*E*), 164.310(a)(2)(*i*), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 9.7#3.2; NIST SP: 800-34

**Related Controls Requirement(s):** *AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11*

### ASSESSMENT PROCEDURE: CP-2.1

#### Assessment Objective

Determine if:

(i) the organization develops a contingency plan for the information system that:

- identifies essential missions and business functions and associated contingency requirements;
- provides recovery objectives, restoration priorities, and metrics;
- addresses contingency roles, responsibilities, assigned individuals with contact information;
- addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- addresses eventual, full information system restoration without deterioration of the security *safeguards* originally planned and implemented;
- is reviewed and approved by designated officials within the organization;

(ii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.

#### Assessment Methods And Objects

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

### ASSESSMENT PROCEDURE: CP-2.2

#### Assessment Objective

Determine if:

(i) the organization coordinates contingency planning activities with incident handling activities;

(ii) the organization updates the contingency plan for the information system in accordance with the organization-defined frequency;

(iii) the organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution or testing;

(iv) the organization communicates contingency plan changes to the key contingency personnel and organizational elements.

(v) the organization protects the contingency plan from unauthorized disclosure and modification.

(vi) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).

#### Assessment Methods And Objects

**Examine:** Contingency planning policy; procedures addressing contingency operations for the information system; contingency



*plan; security plan; other relevant documents or records.*

**CP-3 – Contingency Training (Low)**

**Assurance - P2**

**Control**

The organization *provides contingency training to* operational and support personnel (including managers and information system users) *consistent with assigned* roles and responsibilities:

- a. Within ninety (90) days of assuming a contingency role or responsibility;*
- b. When required by* information system *changes;* and
- c. Within every three hundred sixty-five (365) days thereafter.*

**Guidance**

*Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan.*

Managers, responsible for contingency operations, and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirmed that appropriate training has been completed.

**Reference(s):** FISCAM: *AS-5*, CP-2; *HIPAA: 164.308(a)(7)(ii)(D)*; HSPD 7: G(22)(i); *NIST SP: 800-16, 800-50*

**Related Controls Requirement(s):** *AT-2, AT-3, CP-2, IR-2*

**ASSESSMENT PROCEDURE: CP-3.1**

**Assessment Objective**

Determine if:

- (i) the organization provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned* roles and responsibilities;
- (ii) the organization defines in the security plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is no more than every 365 days.*
- (iii) the organization provides refresher training in accordance with organization-defined frequency.*

## Assessment Methods And Objects

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

### CP-4 – Contingency Plan Testing (Low)

*Assurance - P2*

#### Control

The organization:

- a. Tests the contingency plan for the information system within every three hundred sixty-five (365) days using *NIST or CMS* defined tests and exercises, such as the tabletop test in accordance with the current CMS contingency plan procedure to determine the effectiveness *of the plan* and the organizational readiness to execute the plan;
- b. Reviews the contingency plan test results; *and*
- c. *Initiates* corrective actions, *if needed*.

#### **Implementation Standard(s)**

1. *(For CSP only) For service providers, the organization tests and/or exercises the contingency plan for the information system at least every three (3) years using classroom exercises/table top written tests to determine the plan's effectiveness and the organization's readiness to execute the plan.*

#### Guidance

Methods for testing contingency plans to *determine the effectiveness of the plans and to* identify potential weaknesses *in the plans include, for example*, walk-through *and* tabletop *exercises, checklists, simulations* (parallel, full interrupt), *and comprehensive exercises. Organizations conduct* testing *based on the continuity requirements in contingency plans* and include a determination of the effects on *organizational* operations, assets, and individuals arising due to contingency operations. *Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.*

**Reference(s):** *FIPS Pub: 199; FISCAM: AS-5, CP-4; HIPAA: 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 9.7#3.1; NIST SP: 800-34, 800-84*

**Related Controls Requirement(s):** *CP-2, CP-3, IR-3*

### ASSESSMENT PROCEDURE: CP-4.1

#### Assessment Objective

Determine if:

- (i) the organization defines in the security plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted;
- (ii) the organization defines in the security plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is *in accordance with organization-defined frequency*;

- (iii) the organization tests the contingency plan using organization-defined tests *and* exercises in accordance with organization-defined frequency;
- (iv) the organization reviews the contingency plan test/exercise results and takes corrective actions.
- (v) *(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

#### Assessment Methods And Objects

**Examine:** Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.

#### CP-7 – *Alternate Processing Site* (Low)

*PI*

#### Control

*The organization:*

- a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; and*
- b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and*
- c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.*

#### **Implementation Standard(s)**

- 1. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of system Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs).*
- 2. (For CSP only) For service providers, the organization defines a resumption time period consistent with the recovery time objectives and business impact analysis. The time period is approved and accepted by the Joint Authorization Board (JAB).*

#### **Guidance**

*Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.*

*Equipment and supplies required to resume operations within the CMS-defined 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*

<i>with CMS recovery time objectives.</i>	
<b>Reference(s):</b> FISCAM: AS-5, CP-2; HIPAA: 164.308(a)(7)(ii)(B), 164.310(a)(2)(i); IRS-1075: 4.7.3#2, 9.7#3.4; NIST SP: 800-34	<b>Related Controls Requirement(s):</b> CP-2, CP-6, CP-8, CP-9, CP-10, MA-6
<b>ASSESSMENT PROCEDURE: CP-7.1</b>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization establishes an alternate processing site;</i></li> <li><i>(ii) the organization includes necessary alternate processing site agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the organization-defined time period;</i></li> <li><i>(iii) the organization ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption;</i></li> <li><i>(iv) the organization ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.</i></li> <li><i>(v) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><i><b>Examine:</b> Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; security plan; spare equipment and supplies at alternate processing site; equipment and supply contracts; service level agreements; other relevant documents or records.</i></p>	
<b>CP-9 – Information System Backup (Low)</b>	
<b>Control</b>	
<p>The organization:</p> <ul style="list-style-type: none"> <li>a. Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;</li> <li>b. Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;</li> <li>c. Conducts backups of information system documentation including security-related documentation and other forms of data, including paper records <i>within the defined frequency (defined in the applicable security plan) consistent with recovery time and recovery point objectives</i>; and</li> <li>d. Protects the confidentiality, integrity, <i>and availability</i> of backup information at storage locations.</li> </ul>	

**Implementation Standard(s)**

1. Perform backups of user-level and system-level information (including system state information) every month.
3. *(For CSP only) For service providers, these Standards replace the above Control and Standard. The organization shall determine what elements of the cloud environment require the Information System Backup control. The cloud environment elements requiring Information System Backup are approved and accepted by the Joint Authorization Board (JAB).*
4. *(For CSP only) For service providers, the organization determines how Information System Backup is going to be verified and appropriate periodicity of the check. The verification and periodicity of the Information System Backup are approved and accepted by the Joint Authorization Board (JAB).*
5. *(For CSP only) For service providers, the organization:*
  - a. *Conducts backups of user-level information contained in the information system daily incremental; weekly full;*
  - b. *Conducts backups of system-level information contained in the information system daily incremental; weekly full;*
  - c. *Conducts backups of information system documentation including security-related documentation daily incremental; weekly full.*
6. *(For CSP only) For service providers, the organization maintains at least three (3) backup copies of user-level information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the Joint Authorization Board (JAB).*
7. *(For CSP only) For service providers, the organization maintains at least three (3) backup copies of system-level information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the Joint Authorization Board (JAB).*
8. *(For CSP only) For service providers, the organization maintains at least three (3) backup copies of information system documentation including security information (at least one (1) of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the Joint Authorization Board (JAB).*

**Guidance**

System-level information includes, for example, system-state information, operating system and application software, and licenses. *User-level information includes any information other than system-level information. Mechanisms* employed by organizations to protect the integrity of information system backups *include, for example, digital signatures and cryptographic hashes.* Protection of system backup information while in transit is beyond the scope of this control. *Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.*

The transfer rate of backup information to an alternate storage site (if so designated) is guided by the CMS recovery time objectives and recovery point objectives. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time.

**Reference(s):** FISCAM: AS-5, CP-2; HIPAA: 164.308(a)(7)(ii)(A),

**Related Controls Requirement(s):** *CP-2,*

<p>164.308(a)(7)(ii)(B), 164.310(d)(2)(iv), 164.312(c)(1); IRS-1075: 9.7#3.5; NIST SP: 800-34</p>	<p>CP-6, MP-4, MP-5, SC-13</p>
<p><b>ASSESSMENT PROCEDURE: CP-9.1</b></p>	
<p><b>Assessment Objective</b>  Determine if:  <i>(i) the organization backs up user-level information in accordance with the frequency specified in Implementation Standard 1;</i>  <i>(ii) the organization backs up system-level information in accordance with the frequency specified in Implementation Standard 1;</i>  <i>(iii) the organization backs up information system documentation (including security-related information and other forms of data).</i>  <i>(iv) the organization protects the confidentiality, integrity, and availability of backup information at storage locations</i>  <i>(v) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></p> <p><b>Assessment Methods And Objects</b>  <b>Examine:</b> Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; backup storage location(s); information system backup logs or records; other relevant documents or records.</p>	
<p><b>ASSESSMENT PROCEDURE: CP-9.2</b></p>	
<p><b>Assessment Objective</b>  Determine if the organization protects the confidentiality and integrity of backup information at the storage location.</p> <p><b>Assessment Methods And Objects</b>  <b>Examine:</b> Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; information system configuration settings and associated documentation; backup storage location(s); other relevant documents or records.</p>	
<p><b>CP-10 – Information System Recovery and Reconstitution (Low)</b></p>	
<p><b>Control</b>  The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.</p> <p><b>Implementation Standard(s)</b>  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,</p>	

- (c) Reestablish configuration settings,
- (d) Reinstall application and system software, and
- (e) Fully test the system.

#### Guidance

Recovery is executing information system contingency plan activities to restore CMS missions/business functions. Reconstitution takes place following recovery and includes activities for returning *organizational* information systems to *fully operational states*. Recovery and reconstitution *operations reflect mission and business* priorities, recovery point/time and reconstitution objectives, and *established organizational* metrics *consistent with contingency plan requirements*. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes *assessments* of fully restored information system *capabilities, reestablishment of continuous monitoring activities*, potential *information* system reauthorizations, and activities to prepare the systems against *future disruptions, compromises*, or failures. Recovery/reconstitution capabilities employed by *organizations* can *include both* automated mechanisms and manual procedures.

**Reference(s):** FISCAM: *AS-5*, CP-2; HIPAA: 164.308(a)(7)(ii)(*B*), *164.308(a)(7)(ii)(C)*; HSPD 7: G(22)(i); *NIST SP: 800-34*

**Related Controls Requirement(s):** *CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24*

#### ASSESSMENT PROCEDURE: CP-10.1

##### Assessment Objective

Determine if:

- (i)* the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure;
- (ii)* the organization provides for the recovery of the information system after a failure or other contingency in a trusted, secure, and verifiable manner.
- (iii)* the organization meets all the requirements specified in the applicable Implementation Standard(s).

##### Assessment Methods And Objects

**Examine:** Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.



## 7.0 IDENTIFICATION AND AUTHENTICATION (IA)

*Error! Reference source not found.*

IA-1 – Identification and Authentication Policy and Procedures (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. Identification and authentication policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. Identification and authentication procedures within every three hundred sixty-five (365) days.</i></li> </ol>		
<b>Guidance</b> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>IA</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing policy and procedures</i>.</p>		
<b>Reference(s):</b> <i>FIPS Pub: 201; FISCAM: AS-1, SM-1, SM-3; IRS-1075: 9.8#1.1; NIST SP: 800-12, 800-63, 800-73, 800-76, 800-78, 800-100</i>		<b>Related Controls Requirement(s):</b> <i>PM-9</i>
<b>ASSESSMENT PROCEDURE: IA-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <p><i>(i) the organization develops and documents identification and authentication policy;</i></p> <p><i>(ii) the organization identification and authentication policy addresses:</i></p> <ul style="list-style-type: none"> <li><i>- purpose;</i></li> <li><i>- scope;</i></li> </ul>		



- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented identification and authentication policy to *applicable personnel* within the organization having associated identification and authentication roles and responsibilities;

(iv) the organization develops and documents identification and authentication procedures;

(v) the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls;

(vi) the organization disseminates documented identification and authentication procedures to *applicable personnel* within the organization having associated identification and authentication roles and responsibilities;

(vii) the organization reviews *and* updates the identification and authentication policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

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

#### IA-2 – Identification and Authentication (Organizational Users) (Low)

*PI*

##### Control

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

##### Implementation Standard(s)

1. Require the use of system and/or network authenticators and unique user identifiers.
2. Help desk support requires user identification for any transaction that has information security implications.

##### Guidance

Organizational users include employees or individuals *that organizations deem* to have equivalent status of employees (e.g., contractors, guest researchers). *This control applies to* all accesses other than: (i) accesses *that are* explicitly identified and documented in AC-14; *and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require* unique identification of individuals in group accounts (e.g., shared privilege accounts) *or* for detailed accountability of *individual* activity. *Organizations employ* passwords, tokens, *or* biometrics *to authenticate user identities*, or in the case multifactor authentication, *or* some combination thereof. Access to *organizational* information systems is defined as either local *access* or network *access*. Local access is any access to *organizational* information systems by *users* (or

processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8.

**Reference(s):** *FIPS Pub: 201; FISCAM: AC-2, AS-2; HIPAA: 164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d); IRS-1075: 9.3#2.3, 9.8#1.2; NIST SP: 800-63, 800-73, 800-76, 800-78; OMB: M-04-04, M-06-16, M-11-11; Web: idmanagement.gov*

**Related Controls Requirement(s):** AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8

#### ASSESSMENT PROCEDURE: IA-2.1

##### Assessment Objective

Determine if:

- (i) the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
- (ii) the organization meets all the requirements specified in the applicable Implementation Standard(s).

##### Assessment Methods And Objects

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

<b>IA-2(1) - <i>Network Access to Privileged Accounts</i> – Enhancement (Low)</b>		<b>PI</b>
<b>Control</b>		
The information system <i>implements</i> multifactor authentication for network access to privileged accounts.		
<b>Reference(s):</b> <i>IRS-1075: 9.8#1.2</i>		<b>Related Controls Requirement(s):</b> <i>AC-6</i>
<b>ASSESSMENT PROCEDURE: IA-2(1).1</b>		
<b>Assessment Objective</b>		
Determine if:		
(i) the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;		
(ii) the information system <i>implements</i> multifactor authentication for network access to privileged accounts.		
<b>Assessment Methods And Objects</b>		
<b>Examine:</b> Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records.		
<b>IA-2(12) - <i>Acceptance of PIV Credentials</i> – Enhancement (Low)</b>		<b>PI</b>
<b>Control</b>		
<i>The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.</i>		
<b>Guidance</b>		
<i>This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.</i>		
<b>Reference(s):</b>		<b>Related Controls Requirement(s):</b> <i>AU-2, PE-3, SA-4</i>
<b>ASSESSMENT PROCEDURE: IA-2(12).1</b>		
<b>Assessment Objective</b>		
<i>Determine if the information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.</i>		
<b>Assessment Methods And Objects</b>		
<b>Examine:</b> <i>Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents</i>		

*or records.*

***Test:** Automated mechanisms implementing PIV credential capability for the information system.*

#### IA-4 – Identifier Management (Low)

**PI**

##### Control

The organization manages information system identifiers by:

- Receiving authorization from *defined personnel or roles (defined in the applicable security plan)* to assign *an individual, group, role, or device identifier*;
- Selecting an identifier that identifies an individual, *group, role, or device*;
- Assigning the identifier to the intended *individual, group, role, or device*;
- Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three *(3) years* has expired; and
- Disabling the identifier after *sixty (60) days or less* of inactivity and deleting disabled accounts during the annual re-certification process.

##### Implementation Standard(s)

- (For CSP only) For service providers, the organization prevents reuse of user or device identifiers for at least two (2) years and disables the user identifier after ninety (90) days of inactivity.*
- (For CSP only) For service providers, the organization defines time period of inactivity for device identifiers. The time period is approved and accepted by Joint Authorization Board (JAB).*

##### Guidance

Common device identifiers include, *for example*, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of *individual* identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). *Typically, individual identifiers are the user names of the information system accounts assigned to those individuals.* In such instances, the account management activities of AC-2 *use account names provided by IA-4. This control also addresses individual* identifiers not necessarily associated with information system accounts (e.g., *identifiers* used in physical security control databases accessed by badge reader systems for access to information *systems*). *Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.*

**Reference(s):** *FIPS Pub: 201; FISCAM: AC-2, AS-2; HIPAA: 164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d); IRS-1075: 9.8#2; NIST SP: 800-73, 800-76, 800-78*

**Related Controls Requirement(s):** *AC-2, IA-2, IA-3, IA-5, IA-8, SC-37*

## ASSESSMENT PROCEDURE: IA-4.1

### Assessment Objective

Determine if:

(i) the organization manages information system identifiers by:

- receiving authorization from *defined personnel or roles (defined in the applicable security plan)* to assign *an individual, group, role, or device identifier*;
- selecting an identifier that identifies an individual, *group, role, or device*;
- assigning the identifier to the intended *individual, group, role, or device*;
- preventing reuse of identifiers for the organization-defined time period;
- disabling the identifier after the organization-defined time period of inactivity;

(ii) the organization defines in the security plan, explicitly or by reference, the time period of inactivity after which a user identifier is to be disabled.

(iii) *(For CSP only)* the organization meets all the requirements specified in the applicable Implementation Standard(s).

### Assessment Methods And Objects

**Examine:** Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records.

## IA-5 – Authenticator Management (Low)

**PI**

### Control

*Non-standard account-authenticator management specifications are addressed in the CMS Risk Management Handbook (RMH), Volume III, Standard 4.3, “Non-Standard Authenticator Management”. For all others,* the organization manages information system authenticators by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, *group, role, or device* receiving the authenticator;
- b. Establishing initial authenticator content for authenticators defined by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators *prior to* information system installation;
- f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing authenticators as *follows*:

- *Passwords are valid for no longer than the period directed in IA-5(1);*

- *PIV compliant access cards are valid for no longer than five (5) years; and*

- *PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years;*

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring *individuals* to take, and having devices implement, specific *security safeguards* to *protect* authenticators; *and*

*j. Changing authenticators for group/role accounts when membership to those accounts changes.*

**Implementation Standard(s)**

*1. (For CSP only) For service providers, the organization manages information system authenticators for users and devices by changing/refreshing authenticators every sixty (60) days by authenticator type.*

**Guidance**

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

**Reference(s):** *FIPS Pub: 201; FISCAM: AC-2, AS-2; HIPAA: 164.308(a)(5)(ii)(D); IRS-1075: 9.8#2; NIST SP: 800-63, 800-73, 800-76, 800-78; OMB: M-04-04, M-11-11; Web: idmanagement.gov*

**Related Controls Requirement(s):** *AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28*

## ASSESSMENT PROCEDURE: IA-5.1

### Assessment Objective

*Determine if:*

(i) the organization manages information system authenticators by:

- verifying, as part of the initial authenticator distribution, the identity of the individual, *group, role*, or device receiving the authenticator;
- establishing initial authenticator content for authenticators defined by the organization;
- ensuring that authenticators have sufficient strength of mechanism for their intended use;
- establishing and implementing administrative procedures for initial authenticator distribution;
- establishing and implementing administrative procedures for lost/compromised or damaged authenticators;
- establishing and implementing administrative procedures for revoking authenticators;
- changing default content of authenticators *prior to* information system installation;
- establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;
- protecting authenticator content from unauthorized disclosure and modification;
- requiring *individuals* to take, and having devices implement, specific *security safeguards* to *protect* authenticators;
- *changing authenticators for group/role accounts when membership to those accounts changes.*

(ii) *(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

### Assessment Methods And Objects

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

## IA-5(1) - Password-Based Authentication – Enhancement (Low)

*P1*

### Control

*Non-standard account-authenticator management specifications are addressed in the CMS Risk Management Handbook (RMH), Volume III, Standard 4.3, “Non-Standard Authenticator Management”. For all other password-based authentication, the information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent:*

- a. Prohibits the use of dictionary names or words;*
- b. Enforces at least the following minimum password requirements (User/Privileged/Process [acting on behalf of a User]):*
  - *MinimumPasswordAge = 1/1/1;*



- *MaximumPasswordAge = 60/60/120;*
- *MinimumPasswordLength = 8/8/15;*
- *PasswordComplexity = minimum (1/1/3) character from the four (4) character categories (A-Z, a-z, 0-9, special characters; and*
- *PasswordHistorySize = 6/6/12;*
- c. If the operating environment allows, enforces a minimum of (4/4/8) changed characters when new passwords are created;*
- d. Stores and transmits only encrypted representations of passwords; and*
- e. Allows the use of a temporary password for system logons with an immediate change to a permanent password.*

**Implementation Standard(s)**

- 1. (For CSP only) For service providers, this Standard replaces the above Enhancement. The information system, for password-based authentication:*
- (a) Enforces minimum password complexity of case sensitive, minimum of twelve (12) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters;*
  - (b) Enforces at least one (1) changed character or as determined by the information system (where possible) when new passwords are created;*
  - (c) Encrypts passwords in storage and in transmission;*
  - (d) Enforces password minimum and maximum lifetime restrictions of one (1) day minimum, sixty (60) days maximum; and*
  - (e) Prohibits password reuse for twenty four (24) generations.*

**Guidance**

This control enhancement *applies to* single-factor *authentication of individuals using passwords as individual or group authenticators, and* in a similar manner, *when passwords are part of multifactor authenticators. This control* enhancement does not apply *when* passwords are used to unlock hardware authenticators (*e.g., Personal Identity Verification cards*). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. *Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. (For CSP only) Mobile devices are excluded from the password complexity requirement.*

<b>Reference(s):</b>	<b>Related Controls Requirement(s):</b> <i>IA-6</i>
<b>ASSESSMENT PROCEDURE: IA-5(1).1</b>	
<b>Assessment Objective</b>	
Determine if:	
<i>(i) the information system, for password-based authentication:</i>	

- enforces the minimum password complexity standards that meet the organization-defined requirements;
- enforces the organization-defined minimum number of characters that must be changed when new passwords are created;
- encrypts passwords in storage and in transmission;
- enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters;
- prohibits password reuse for the organization-defined number of generations.

*(ii) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

#### **Assessment Methods And Objects**

**Examine:** Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

#### **IA-5(11) - Hardware Token-Based Authentication – Enhancement (Low)**

**PI**

##### **Control**

*The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in the Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.*

##### **Guidance**

*Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.*

##### **Reference(s):**

##### **Related Controls Requirement(s):**

#### **ASSESSMENT PROCEDURE: IA-5(11).1**

##### **Assessment Objective**

*Determine if the information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in the Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.*

##### **Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; other relevant documents or records.

#### **IA-6 – Authenticator Feedback (Low)**

**PI**

##### **Control**

The information system obscures feedback of authentication information during the authentication process to protect the

information from possible exploitation/use by unauthorized individuals.	
<b>Guidance</b> <p>The feedback from information systems does not provide information that would allow unauthorized <i>individuals</i> to compromise authentication <i>mechanisms</i>. <i>For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.</i></p>	
<b>Reference(s):</b> FISCAM: AC-2, AS-2; HIPAA: 164.308(a)(5)(ii)(D); IRS-1075: 9.8#1.2	<b>Related Controls Requirement(s):</b> PE-18
<b>ASSESSMENT PROCEDURE: IA-6.1</b>	
<b>Assessment Objective</b> <p>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.</p>	
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.</p>	
<b>IA-7 – Cryptographic Module Authentication (Low)</b>	
<b>Control</b>	
<p>The information system <i>implements</i> mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.</p>	
<b>Guidance</b> <p><i>Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.</i></p>	
<b>Reference(s):</b> FIPS Pub: 140; FISCAM: AC-4, AS-2; HIPAA: 164.308(a)(5)(ii)(D); Web: <a href="http://csrc.nist.gov/groups/STM/cmvp/index.html">csrc.nist.gov/groups/STM/cmvp/index.html</a>	<b>Related Controls Requirement(s):</b> SC-12, SC-13

<b>ASSESSMENT PROCEDURE: IA-7.1</b>	
<b>Assessment Objective</b> Determine if the information system <i>implements</i> mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	
<b>Assessment Methods And Objects</b> <b>Examine:</b> Identification and authentication policy; procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.	
<b>IA-8 – Identification and Authentication (Non-Organizational Users) (Low)</b>	
<b>Control</b>	
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	
<b>Guidance</b>	
Non-organizational users include information system users other than organizational users explicitly covered by IA-2. <i>These individuals</i> are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). <i>Organizations use risk assessments to determine</i> authentication needs <i>and consider</i> scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. <i>IA-2 addresses</i> identification and authentication requirements for <i>access to</i> information <i>systems</i> by organizational users. If E-Authentication is used, refer to <i>Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards</i> .	
<b>Reference(s):</b> <i>NIST SP: 800-63, 800-116; OMB: M-04-04, M-10-06-2011, M-11-11; Web: idmanagement.gov</i>	<b>Related Controls Requirement(s):</b> <i>AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-9</i>
<b>ASSESSMENT PROCEDURE: IA-8.1</b>	
<b>Assessment Objective</b> Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf	

of non-organizational users).

**Assessment Methods And Objects**

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

**IA-8(1) - Acceptance of PIV Credentials from Other Agencies – Enhancement (Low)**

**PI**

**Control**

*The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.*

**Guidance**

*This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.*

**Reference(s):**

**Related Controls Requirement(s):** AU-2, PE-3, SA-4

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

**Assessment Objective**

*Determine if the information system accepts and electronically verifies PIV credentials from other federal agencies.*

**Assessment Methods And Objects**

**Examine:** Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; PIV credential documentation; other relevant documents or records.

**IA-8(2) - Acceptance of Third-Party Credentials – Enhancement (Low)**

**PI**

**Control**

*The information system accepts only FICAM-approved third-party credentials.*

**Guidance**

*This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved*

<i>by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.</i>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s): AU-2</b>
<b>ASSESSMENT PROCEDURE: IA-8(2).1</b>	
<b>Assessment Objective</b> <i>Determine if the information system accepts only FICAM-approved third-party credentials.</i>	
<b>Assessment Methods And Objects</b> <i><b>Examine:</b> Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; FICAM credential documentation; other relevant documents or records.</i>	
<b>IA-8(3) - Use of FICAM-Approved Products – Enhancement (Low)</b>	
<b>PI</b>	
<b>Control</b> <i>The organization employs only FICAM-approved information system components in information systems that authenticate non-organizational users and accept third-party credentials.</i>	
<b>Guidance</b> <i>This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program.</i>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s): SA-4</b>
<b>ASSESSMENT PROCEDURE: IA-8(3).1</b>	
<b>Assessment Objective</b> <i>Determine if the organization employs only FICAM-approved information system components in information systems that authenticate non-organizational users and accept third-party credentials.</i>	
<b>Assessment Methods And Objects</b> <i><b>Examine:</b> Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; FICAM-approved information system component procedures; other relevant documents or records.</i>	

<b>IA-8(4) - Use of FICAM-Issued Profiles – Enhancement (Low)</b>		<b>P1</b>
<b>Control</b>		
<i>The information system conforms to FICAM-issued profiles.</i>		
<b>Guidance</b>		
<i>This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange).</i>		
<b>Reference(s):</b>		<b>Related Controls Requirement(s): SA-4</b>
<b>ASSESSMENT PROCEDURE: IA-8(4).1</b>		
<b>Assessment Objective</b>		
<i>Determine if the information system conforms to FICAM-issued profiles.</i>		
<b>Assessment Methods And Objects</b>		
<i><b>Examine:</b> Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; FICAM-issued credential documentation; other relevant documents or records.</i>		

## 8.0 INCIDENT RESPONSE (IR)

*Error! Reference source not found.*

<b>IR-1 – Incident Response Policy and Procedures (Low)</b>		<b>Assurance - P1</b>
<b>Control</b> <p><i>The organization:</i></p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. Incident response policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. Incident response procedures within every three hundred sixty-five (365) days.</i></li> </ol>		
<b>Guidance</b> <p><i>This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.</i></p>		
<b>Reference(s):</b> FISCAM: AC-5, AS-1, AS-2, SM-1, SM-3; HIPAA: 164.308(a)(6)(i); IRS-1075: 9.9#1; NIST SP: 800-12, 800-61, 800-83, 800-100		<b>Related Controls Requirement(s):</b> PM-9
<b>ASSESSMENT PROCEDURE: IR-1.1</b>		
<b>Assessment Objective</b> <p><i>Determine if:</i></p> <p><i>(i) the organization develops and documents incident response policy;</i></p> <p><i>(ii) the organization incident response policy addresses:</i></p> <ul style="list-style-type: none"> <li><i>- purpose;</i></li> <li><i>- scope;</i></li> <li><i>- roles and responsibilities;</i></li> </ul>		



- *management commitment;*
- *coordination among organizational entities;*
- *compliance;*
- (iii) *the organization disseminates documented incident response policy to applicable personnel within the organization having associated incident response roles and responsibilities;*
- (iv) *the organization develops and documents incident response procedures;*
- (v) *the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls;*
- (vi) *the organization disseminates documented incident response procedures to applicable personnel within the organization having associated incident response roles and responsibilities;*
- (vii) *the organization reviews and updates the incident response policy and procedures within every three hundred sixty-five (365) days.*

**Assessment Methods And Objects**

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

**IR-2 – Incident Response Training (Low)**

**Assurance - P2**

**Control**

The organization *provides* incident response *training to information system users consistent with assigned roles and responsibilities:*

- a. Within ninety (90) days of assuming an incident response role or responsibility;*
- b. When required by information system changes; and*
- c. Within every three hundred sixty-five (365) days thereafter.*

**Guidance**

*Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.*

**Reference(s):** FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(6)(i); IRS-1075: 9.9#2.1-2;  
NIST SP: 800-16, 800-50

**Related Controls Requirement(s):** AT-3,  
CP-3, IR-8

## ASSESSMENT PROCEDURE: IR-2.1

### Assessment Objective

*Determine if:*

- (i) the organization *identifies personnel with* incident response roles and responsibilities *with respect to the information system*;
- (ii) the organization *provides* incident response *training to information system users consistent with assigned* roles and responsibilities;
- (iii) incident response *training material addresses the* procedures *and activities necessary to fulfill identified organizational* incident response *roles and responsibilities*;
- (iv) the organization *defines in the security plan, explicitly or by reference, the frequency of refresher* incident response *training in accordance with* organization-defined frequency;
- (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; security plan; incident response plan; incident response training records*; other relevant documents or records.

## IR-4 – Incident *Handling* (Low)

*PI*

### Control

The organization:

- a. *Implements an incident handling capability using the current Risk Management Handbook (RMH), Volume II, Procedure 7.2, Incident Handling*;
- b. *Coordinates incident handling activities with contingency planning activities; and*
- c. *Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.*

#### **Implementation Standard(s)**

- 1. *Document relevant information related to a security incident according to the current Risk Management Handbook (RMH), Volume II, Procedure 7.2, Incident Handling.*
- 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.*

*4. (For CSP only) For service providers, the organization ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.*

#### Guidance

*Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).*

**Reference(s):** *Executive Order: 13587*; FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(6)(ii); IRS-1075: 9.9#1, 9.9#2.3; NIST SP: 800-61

**Related Controls Requirement(s):** AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7

#### 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;
- recovery;

(ii) the organization coordinates incident handling activities with contingency planning activities;

(iii) the organization incorporates lessons learned from ongoing incident handling activities into:

- incident response procedures;
- training;
- testing/exercises;

(iv) the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.

(v) the organization meets all the requirements specified in the applicable Implementation Standard(s).

### Assessment Methods And Objects

**Examine:** Incident response policy; procedures addressing incident handling; incident response plan; other relevant documents or records.

### IR-5 – Incident Monitoring (Low)

*Assurance - PI*

#### Control

The organization tracks and documents information system security incidents.

#### Guidance

Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

**Reference(s):** FISCAM: AC-5, *AS-2*; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(6)(ii); IRS-1075: 9.9#2.3; *NIST SP: 800-61*

**Related Controls Requirement(s):** *AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7*

### ASSESSMENT PROCEDURE: IR-5.1

#### Assessment Objective

Determine if the organization tracks and documents information system security incidents.

#### Assessment Methods And Objects

**Examine:** Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; other relevant documents or records.

### IR-6 – Incident Reporting (Low)

*PI*

#### Control

The organization:

- Requires personnel to report suspected security incidents to the organizational incident response capability within *the* timeframe established in the current *Risk Management Handbook (RMH), Volume II, Procedure 7.2*, Incident Handling; and
- Reports security incident information to designated authorities.

#### **Implementation Standard(s)**

*1. (For CSP only) For service providers, this Standard replaces the above Control. The organization requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended).*

<b>Guidance</b> <p>The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. <i>Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code.</i> The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Current federal policy</i> requires that <i>all federal agencies (unless specifically exempted from such requirements) report</i> security incidents to the <i>United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.</i>  <i>For more information see the see the Risk Management Handbook (RMH), Volume III, Standard 7.1, Incident Handling and Breach Notification.</i></p>		
<b>Reference(s):</b> FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(6)(ii), 164.314(a)(2)(i); NIST SP: 800-61; Web: us-cert.gov		<b>Related Controls Requirement(s):</b> IR-4, IR-5, IR-8
<b>ASSESSMENT PROCEDURE: IR-6.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current <i>Risk Management Handbook (RMH), Volume II, Procedure 7.2</i>, Incident Handling;</li> <li>(ii) the organization reports security incident information to designated authorities.</li> <li>(iii) <i>(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul>		
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records.</p>		
<b>IR-7 – Incident Response Assistance (Low)</b>		<b>P3</b>
<b>Control</b> <p>The organization <i>provides</i> an incident response <i>support resource, integral to</i> the <i>organizational</i> incident response capability <i>that offers advice</i> and <i>assistance to users</i> of the <i>information system for the handling and reporting of security</i> incidents.</p>		
<b>Guidance</b> <p><i>Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. The CMS CISO is available for assistance at mailto:CISO@cms.hhs.gov.</i></p>		

<b>Reference(s):</b> <i>FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(6)(ii)</i>	<b>Related Controls Requirement(s):</b> <i>AT-2, IR-4, IR-6, IR-8, SA-9</i>
<b>ASSESSMENT PROCEDURE: IR-7.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <p><i>(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;</i></p> <p><i>(ii) the incident response support resource is an integral part of the organization's incident response capability.</i></p> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.</p>	
<i><b>IR-8 – Incident Response Plan (Low)</b></i>	<i><b>PI</b></i>
<p><b>Control</b></p> <p>The organization:</p> <p><i>a. Develops an incident response plan that:</i></p> <ol style="list-style-type: none"> <li><i>1. Provides the organization with a roadmap for implementing its incident response capability;</i></li> <li><i>2. Describes the structure and organization of the incident response capability;</i></li> <li><i>3. Provides a high-level approach for how the incident response capability fits into the overall organization;</i></li> <li><i>4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;</i></li> <li><i>5. Defines reportable incidents;</i></li> <li><i>6. Provides metrics for measuring the incident response capability within the organization;</i></li> <li><i>7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and</i></li> <li><i>8. Is reviewed and approved by the applicable Incident Response Team Leader;</i></li> </ol> <p><i>b. Distributes copies of the incident response plan to:</i></p> <ul style="list-style-type: none"> <li><i>- CMS Chief Information Security Officer;</i></li> <li><i>- CMS Chief Information Officer;</i></li> <li><i>- Information System Security Officer;</i></li> <li><i>- CMS Office of the Inspector General/Computer Crimes Unit;</i></li> <li><i>- All personnel within the organization Incident Response Team;</i></li> <li><i>- All personnel within the PII Breach Response Team; and</i></li> <li><i>- All personnel within the organization Operations Centers;</i></li> </ul>	

- c. Reviews the incident response plan within every three hundred sixty-five (365) days;
- d. *Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;*
- e. *Communicates incident response plan changes to the organizational elements listed in b. above; and*
- f. *Protects the incident response plan from unauthorized disclosure and modification.*

**Implementation Standard(s)**

- 1. *(For CSP only) For service providers, the organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements to distribute the response plan to. The incident response list includes designated FedRAMP personnel.*
- 2. *(For CSP only) For service providers, the organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements to communicate any changes to. The incident response list includes designated FedRAMP personnel.*

**Guidance**

*It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.*

**Reference(s):** NIST SP: 800-61

**Related Controls Requirement(s):** MP-2, MP-4, MP-5

**ASSESSMENT PROCEDURE: IR-8.1**

**Assessment Objective**

- Determine if the organization develops an incident response plan that:*
- *provides the organization with a roadmap for implementing its incident response capability;*
  - *describes the structure and organization of the incident response capability;*
  - *provides a high-level approach for how the incident response capability fits into the overall organization;*
  - *meets the unique requirements of the organization, which relate to mission, size, structure, and functions;*
  - *defines reportable incidents;*
  - *provides metrics for measuring the incident response capability within the organization;*
  - *defines the resources and management support needed to effectively maintain and mature an incident response capability;*
  - *is reviewed and approved by the applicable Incident Response Team Leader.*

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

**ASSESSMENT PROCEDURE: IR-8.2**

**Assessment Objective**

*Determine if:*

- (i) the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;*
- (ii) the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan;*
- (iii) the organization updates the incident response plan in accordance with the organization-defined frequency;*
- (iv) the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;*
- (v) the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.*
- (vi) the organization protects the incident response plan from unauthorized disclosure and modification.*
- (vii) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

**Assessment Methods And Objects**

**Examine:** Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.



## 9.0 MAINTENANCE (MA)

*Error! Reference source not found.*

MA-1 – System Maintenance Policy and Procedures (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li>1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; <i>and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li>1. System maintenance policy within every three hundred sixty-five (365) days; and</li> <li>2. System maintenance procedures within every three hundred sixty-five (365) days.</li> </ol>		
<b>Guidance</b> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>MA</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system-specific</i> policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing</i> policy <i>and procedures</i>.</p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.310(a)(2)(iv); IRS-1075: 9.10#1.1, 9.10#1.2, 9.10#1.3; NIST SP: 800-12, 800-100		<b>Related Controls Requirement(s):</b> PM-9
<b>ASSESSMENT PROCEDURE: MA-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <p><i>(i)</i> the organization develops and documents system maintenance policy;</p> <p><i>(ii)</i> the organization system maintenance policy addresses:</p> <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> <li>- roles and responsibilities;</li> </ul>		

- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented system maintenance policy to *applicable personnel* within the organization having associated system maintenance roles and responsibilities;

(iv) the organization develops and documents system maintenance procedures;

(v) the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls;

(vi) the organization disseminates documented system maintenance procedures to *applicable personnel* within the organization having associated system maintenance roles and responsibilities;

(vii) the organization reviews *and* updates the information system maintenance policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

**Examine:** Information system maintenance policy and procedures; other relevant documents or records.

#### MA-2 – Controlled Maintenance (Low)

**P2**

#### Control

The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. *Approves and monitors* all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that *the applicable Business Owner (or an official designated in the applicable security plan)* explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; *and*

*f. Includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.*

#### Guidance

*This control addresses the information security aspects of the information system maintenance program and applies to all types of*

*maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.*

**Reference(s):** FISCAM: *AS-5*, CP-2; *HIPAA: 164.310(a)(2)(iv)*; IRS-1075: *9.10#1.1*, *9.10#1.2*, *9.10#1.3*

**Related Controls Requirement(s):** *CM-3*, *CM-4*, *MA-4*, *MP-6*, *PE-16*, *SA-12*, *SI-2*

#### **ASSESSMENT PROCEDURE: MA-2.1**

##### **Assessment Objective**

Determine if:

- (i)* the organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- (ii)* the organization *approves and monitors* all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- (iii)* the organization requires that *the applicable Business Owner (or an official designated in the applicable security plan)* explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
- (iv)* the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
- (v)* the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
- (vi) the organization includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.*

##### **Assessment Methods And Objects**

**Examine:** Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records.

MA-4 – <i>Nonlocal</i> Maintenance (Low)		P1
<b>Control</b> <p>The organization <i>monitors and controls nonlocal maintenance and diagnostic activities; and</i> prohibits <i>nonlocal</i> system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. <i>If nonlocal maintenance and diagnostic activities are</i> authorized, the organization:</p> <ul style="list-style-type: none"> <li>a. Allows the use of <i>nonlocal</i> maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;</li> <li><i>b.</i> Employs strong identification and authentication techniques in the establishment of <i>nonlocal</i> maintenance and diagnostic sessions;</li> <li><i>c.</i> Maintains records for <i>nonlocal</i> maintenance and diagnostic activities; and</li> <li><i>d.</i> Terminates all sessions and network connections when <i>nonlocal</i> maintenance is completed.</li> </ul> <b>Implementation Standard(s)</b> <ul style="list-style-type: none"> <li>1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.</li> </ul>		
<b>Guidance</b> <p><i>Nonlocal</i> maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of <i>nonlocal</i> maintenance and diagnostic sessions <i>reflect</i> the network access requirements in IA-2. <i>Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication.</i> Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls.</p>		
<b>Reference(s):</b> <i>FIPS Pub: 140-2, 197, 201; FISCAM: AS-1, SM-7; IRS-1075: 9.10#1.1, 9.10#1.2, 9.10#1.3; NIST SP: 800-63, 800-88</i>		<b>Related Controls Requirement(s):</b> <i>AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17</i>
<b>ASSESSMENT PROCEDURE: MA-4.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization prohibits <i>nonlocal</i> CMS system maintenance unless explicitly authorized, in writing, by the CIO;</li> </ul>		

- (ii) the organization monitors *nonlocal* maintenance and diagnostic activities;
- (iii) if authorized, the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of *nonlocal* maintenance and diagnostic tools;
- (iv) if authorized, the organization allows the use of *nonlocal* maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;
- (v) if authorized, the organization employs strong *authenticators* in the establishment of *nonlocal* maintenance and diagnostic sessions;
- (vi) if authorized, the organization terminates all sessions and network connections when *nonlocal* maintenance is completed.
- (vii) if authorized, the organization maintains records for *nonlocal* maintenance and diagnostic activities;
- (viii) if authorized, the organization (or information system in certain cases) terminates *session* and network connections when *nonlocal* maintenance or diagnostics is completed.
- (ix) the organization meets all the requirements specified in the applicable Implementation Standard(s).

#### Assessment Methods And Objects

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

#### MA-5 – Maintenance Personnel (Low)

*PI*

#### Control

The organization:

- a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
- b. Ensures that *non-escorted* personnel performing maintenance on the information system have required access authorizations;  
*and*
- c. Designates organizational personnel with required access authorizations and technical competence to supervise *the* maintenance activities of personnel *who* do not possess the required access authorizations.

#### Guidance

*This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on*

*and near the systems.* Individuals not previously identified *as authorized maintenance personnel*, such as *information technology manufacturers, vendors, system integrators*, and consultants, may require privileged access to *organizational information systems*, for example, when required to conduct maintenance activities with little or no notice. Based on *organizational assessments* of risk, *organizations* may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

**Reference(s):** FISCAM: *AS-5*, CP-2; *HIPAA: 164.308(a)(3)(ii)(A)*

**Related Controls Requirement(s):** *AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3*

#### **ASSESSMENT PROCEDURE: MA-5.1**

##### **Assessment Objective**

Determine if:

- (i)* the organization establishes a process for maintenance personnel authorization;
- (ii)* the organization maintains a list of authorized maintenance organizations or personnel;
- (iii)* personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence to supervise *the maintenance activities of personnel who do not possess the required access authorization.*

##### **Assessment Methods And Objects**

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

## 10.0 MEDIA PROTECTION (MP)

*Error! Reference source not found.*

MP-1 – Media Protection Policy and Procedures (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li>1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; <i>and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li>1. Media protection policy within every three hundred sixty-five (365) days; and</li> <li>2. Media protection procedures within every three hundred sixty-five (365) days.</li> </ol>		
<b>Guidance</b> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>MP</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing</i> policy <i>and procedures</i>.</p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.310(d)(1); IRS-1075: 3.2#3.2, 3.2#3.3, 4.6#1; NIST SP: 800-12, 800-100		<b>Related Controls Requirement(s):</b> PM-9
<b>ASSESSMENT PROCEDURE: MP-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <p><i>(i)</i> the organization develops and documents media protection policy;</p> <p><i>(ii)</i> the organization media protection policy addresses:</p> <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> <li>- roles and responsibilities;</li> </ul>		



- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented media protection policy to *applicable personnel* within the organization having associated media protection roles and responsibilities;

(iv) the organization develops and documents media protection procedures;

(v) the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls;

(vi) the organization disseminates documented media protection procedures to *applicable personnel* within the organization having associated media protection roles and responsibilities.

(vii) the organization reviews *and* updates the media protection policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

**Examine:** Media protection policy and procedures; other relevant documents or records.

#### MP-2 – Media Access (Low)

*PI*

#### Control

*The organization restricts access to sensitive digital and non-digital media defined within NIST SP 800-88, Guidelines for Media Sanitization, to authorized individuals by disabling:*

- *CD/DVD writers and allowing access to authorized personnel; and*
- *USB ports and allowing access to authorized personnel.*

#### **Implementation Standard(s)**

- 1. (For CSP only) For service providers, this Standard replaces the above Control. The organization defines types of digital and non-digital media. The media types are approved and accepted by the Joint Authorization Board (JAB).*
- 2. (For CSP only) For service providers, the organization defines a list of individuals with authorized access to defined media types. The list of authorized individuals is approved and accepted by the JAB.*
- 3. (For CSP only) For service providers, the organization defines the types of security measures to be used in protecting defined media types. The security measures are approved and accepted by the JAB.*

#### Guidance

Information system media includes both digital *and non-digital media*. *Digital media includes, for example*, diskettes, magnetic tapes, external/removable hard *disk* drives, flash drives, compact disks, *and* digital video disks. *Non-digital media includes, for*

*example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.*

**Reference(s):** *FIPS Pub: 199; FISCAM: AC-4, AS-2; HIPAA: 164.308(a)(3)(ii)(A), 164.310(c), 164.310(d)(1), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1; NIST SP: 800-111*

**Related Controls Requirement(s):** *AC-3, IA-2, MP-4, PE-2, PE-3, PL-2*

## ASSESSMENT PROCEDURE: MP-2.1

### Assessment Objective

Determine if:

*(i) the organization defines:*

- digital and non-digital media requiring restricted access;
- individuals authorized to access the media;
- security measures taken to restrict access;

*(ii) the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures.*

*(iii) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

### Assessment Methods And Objects

**Examine:** Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records.

## MP-6 – Media Sanitization (Low)

*PI*

### Control

The organization:

- a. Sanitizes both digital and non-digital *information system media* prior to disposal, release out of organizational control, or release for reuse *using defined sanitization techniques and procedures (defined in the applicable security plan) in accordance with applicable federal and organizational standards and policies; and*
- b. Employs sanitization mechanisms with *the* strength and integrity commensurate with the *security category or* classification of the information.

### Implementation Standard(s)

1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and

procedures.

### Guidance

This control applies to all *information system media, both digital and non-digital*, subject to disposal or reuse, whether or not *the media is* considered removable. *Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization* process *removes* information from *the* media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, *cryptographic erase*, and *destruction*, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

*Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use* discretion on the employment of *approved* sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on *organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information.*

**Reference(s):** *FIPS Pub: 199; FISCAM: AC-4, AS-2; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii), 164.312(c)(1); IRS-1075: 3.2#1, 3.3#1, 4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2, 8.4#1, 8.4#2, 8.4#3; NIST SP: 800-60, 800-88; Web: [nsa.gov/ia/mitigation\\_guidance/](http://nsa.gov/ia/mitigation_guidance/)*

**Related Controls Requirement(s):** *MA-2, MA-4, RA-3, SC-4*

### ASSESSMENT PROCEDURE: MP-6.1

#### Assessment Objective

Determine if:

*(i) the organization sanitizes both digital and non-digital information system media prior to:*

- disposal;*
- release out of organizational control; or*
- release for reuse;*

*the organization sanitizes both digital and non-digital information system media prior to:*

- disposal;*
- release out of organizational control; or*
- release for reuse;*

*(iii) the organization employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.*

(iv) the organization meets all the requirements specified in the applicable Implementation Standard(s).

(ii) *the organization uses defined sanitization techniques and procedures (defined in the applicable security plan) in accordance with applicable federal and organizational standards and policies to sanitize media;*

#### Assessment Methods And Objects

**Examine:** Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records.

#### MP-7 – Media Use (Low)

**PI**

#### Control

*The organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).*

#### Guidance

*Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.*

**Reference(s):** *FIPS Pub: 199; NIST SP: 800-111*

**Related Controls Requirement(s):** *AC-19, PL-4*

#### ASSESSMENT PROCEDURE: **MP-7.1**

#### Assessment Objective

*Determine if the organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).*

***Assessment Methods And Objects***

***Examine:*** Information system media protection policy; procedures addressing media usage; information system audit records; other relevant documents or records.

## 11.0 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

*Error! Reference source not found.*

<b>PE-1 – Physical and Environmental Protection Policy and Procedures (Low)</b>		<b>Assurance - P1</b>
<b>Control</b>		
<p><i>The organization:</i></p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. Physical and environmental protection policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. Physical and environmental protection procedures within every three hundred sixty-five (365) days.</i></li> </ol>		
<b>Guidance</b>		
<p><i>This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.</i></p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii); IRS-1075: 4.2#6, 4.6#1; NIST SP: 800-12, 800-100		<b>Related Controls Requirement(s):</b> PM-9
<b>ASSESSMENT PROCEDURE: PE-1.1</b>		
<b>Assessment Objective</b>		
<p><i>Determine if:</i></p> <p><i>(i) the organization develops and documents physical and environmental protection policy;</i></p> <p><i>(ii) the organization physical and environmental protection policy addresses:</i></p> <ul style="list-style-type: none"> <li><i>- purpose;</i></li> <li><i>- scope;</i></li> </ul>		

- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented physical and environmental protection policy to applicable personnel within the organization having associated physical and environmental protection roles and responsibilities;

(iv) the organization develops and documents physical and environmental protection procedures;

(v) the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls;

(vi) the organization disseminates documented physical and environmental protection procedures to applicable personnel within the organization having associated physical and environmental protection roles and responsibilities;

(vii) the organization reviews and updates the physical and environmental protection policy and procedures within every three hundred sixty-five (365) days.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy and procedures; other relevant documents or records.

**PE-2 – Physical Access Authorizations (Low)**

**PI**

**Control**

The organization:

- a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
- b. Issues authorization credentials for facility access;
- c. Reviews the access list detailing authorized facility access by individuals in accordance with the frequency specified in Implementation Standard 1; and
- d. Removes individuals from the facility access list when access is no longer required.

**Implementation Standard(s)**

1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every three hundred sixty-five (365) days.
3. (For CSP only) For service providers, the organization reviews and approves the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.



<b>Guidance</b> <i>This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.</i>	
<b>Reference(s):</b> FISCAM: AC-6, AS-2; HIPAA: 164.310(a)(1), 164.310(a)(2)(iii); IRS-1075: 4.2#4, 4.3.1#7, 4.3.2#1, 4.3.2#2, 4.3.2#3	<b>Related Controls Requirement(s):</b> PE-3, PE-4, PS-3
<b>ASSESSMENT PROCEDURE: PE-2.1</b>	
<b>Assessment Objective</b> <i>Determine if:</i> <i>(i) the organization identifies areas within the facility that are publicly accessible;</i> <i>(ii) the organization develops and maintains a list of individuals with authorized access to the facility where the information system resides;</i> <i>(iii) the organization issues authorization credentials (e.g., badges, identification cards, smart cards) for facility access;</i> <i>(iv) the organization reviews the access list detailing authorized facility access by individuals in accordance with the frequency specified in Implementation Standard 1;</i> <i>(v) the organization removes individuals from the facility access list when access is no longer required.</i> <i>(vi) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i>	
<b>Assessment Methods And Objects</b> <b>Examine:</b> Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; other relevant documents or records.	
<b>PE-3 – Physical Access Control (Low)</b>	
<b>Control</b> The organization: a. Enforces physical access authorizations <i>at defined</i> entry/exit points to the facility <i>(defined in the applicable security plan)</i> where the information system resides] <i>by;</i> 1. <i>Verifying</i> individual access authorizations before granting access to the facility; <i>and</i> 2. <i>Controlling ingress/egress</i> to the facility using <i>guards and/or defined physical access control systems/devices (defined in the</i>	

- applicable security plan);*
- b. Maintains physical access audit logs for defined entry/exit points (as defined in the applicable security plan);*
- c. Provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible;*
- d. Escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan);*
- e. Secures keys, combinations, and other physical access devices;*
- f. Inventories defined physical access devices (defined in the applicable security plan) with the frequency specified in Implementation Standard 5; and*
- g. Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every three hundred sixty-five (365) days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.*

**Implementation Standard(s)**

1. Control data center/facility access by use of door and window locks.
2. Store and operate servers in physically secure environments protected from unauthorized access.
- 5. Conducts inventories of physical access devices within every one hundred eighty (180) days.*
- 6. (For CSP only) For service providers, the organization inventories physical access devices at least annually.*

**Guidance**

*This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.*

<p><b>Reference(s):</b> <i>FIPS Pub: 201; FISCAM: AC-6, AS-2; HIPAA: 164.310(a)(1), 164.310(a)(2)(iii), 164.310(b), 164.310(c); IRS-1075: 4.2#2, 4.3#1, 4.3.1#2, 4.3.2#4, 4.3.10#1, 4.3.10#2, 4.3.10#3, 4.6#1; NIST SP: 800-73, 800-76, 800-78, 800-116; Web: fips201ep.cio.gov, idmanagement.gov</i></p>	<p><b>Related Controls Requirement(s):</b> <i>AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3</i></p>
<p><b>ASSESSMENT PROCEDURE: PE-3.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization enforces physical access authorizations <i>at defined</i> entry/exit points to the facility (<i>defined in the applicable security plan</i>) where the information system resides;</li> <li>(ii) the organization verifies individual access authorizations before granting access to the facility;</li> <li>(iii) the organization controls <i>ingress/egress</i> to the facility using <i>guards and/or defined</i> physical access <i>control systems/devices</i> (<i>defined in the applicable security plan</i>);</li> <li>(iv) <i>the organization maintains physical access audit logs for defined entry/exit points (as defined in the applicable security plan);</i></li> <li>(v) <i>the organization provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible;</i></li> <li>(vi) <i>the organization escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan);</i></li> <li>(vii) <i>the organization secures keys, combinations, and other physical access devices;</i></li> <li>(viii) the organization inventories <i>defined</i> physical access devices (<i>defined in the applicable security plan</i>) within <i>the organization-defined frequency</i>;</li> <li>(ix) the organization changes combinations and keys <i>for defined high-risk entry/exit points (defined in the applicable security plan) within the organization-defined frequency</i>; and when keys are lost, <i>and/or when keys are lost</i>, combinations are compromised, or individuals are transferred or terminated.</li> <li>(x) the organization meets all the requirements specified in the applicable Implementation Standard(s).</li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; other relevant documents or records.</p>	

PE-6 – Monitoring Physical Access (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. <i>Monitors</i> physical access to the facility where the information system resides <i>to detect and respond to physical security incidents</i>;</li> <li>b. <i>Reviews physical access logs weekly and upon occurrence of security incidents involving physical security</i>; and</li> <li>c. <i>Coordinates results of reviews and investigations with the organization's incident response capability.</i></li> </ul> <p><b>Implementation Standard(s)</b></p> <ul style="list-style-type: none"> <li>1. <i>(For CSP only) For service providers, the organization reviews physical access logs at least semi-annually.</i></li> </ul>		
<b>Guidance</b> <p><i>Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses.</i></p>		
<b>Reference(s):</b> FISCAM: AC-6, AS-2; HIPAA: 164.310(a)(2)(iii); IRS-1075: 4.3.2#7		<b>Related Controls Requirement(s):</b> CA-7, IR-4, IR-8
<b>ASSESSMENT PROCEDURE: PE-6.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization <i>monitors</i> physical access to the facility where the information system resides <i>to detect and respond to physical security incidents</i>;</li> <li>(ii) <i>the organization reviews physical access logs in accordance with the organization-defined frequency and upon occurrence of security incidents involving physical security</i>;</li> <li>(iii) <i>the organization coordinates results of reviews and investigations with the organization's incident response capability.</i></li> <li>(iv) <i>(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul>		
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> Physical and environmental protection policy; procedures addressing <i>physical</i> access <i>monitoring</i>; <i>security plan</i>; <i>physical</i> access logs or records; other relevant documents or records.</p>		

<b>PE-7 – Visitor Control (Low)</b>		<b>P0</b>
<b>Control</b>		
<i>[Withdrawn: Incorporated into PE-2 and PE-3].</i>		
<b>PE-8 – Visitor Access Records (Low)</b>		<b>Assurance - P3</b>
<b>Control</b>		
<p>The organization:</p> <ul style="list-style-type: none"> <li>a. Maintains visitor access records to the facility where the information system resides <i>for one (1) year</i>; and</li> <li>b. Reviews visitor access records <i>at least</i> monthly.</li> </ul>		
<b>Guidance</b>		
<p>Visitor access records include, for example, <i>names and organizations</i> of <i>persons</i> visiting, visitor <i>signatures, forms</i> of identification, <i>dates</i> of access, entry and departure <i>times, purposes</i> of visits, and <i>names and organizations</i> of persons visited.</p> <p><i>Visitor access records are not required for publicly accessible areas.</i></p>		
<b>Reference(s):</b> FISCAM: AC-6, <i>AS-2; HIPAA: 164.310(a)(2)(iii); IRS-1075: 4.3.1#3, 4.3.1#5, 4.3.2#9, 4.3.2#10</i>		<b>Related Controls Requirement(s):</b>
<b>ASSESSMENT PROCEDURE: PE-8.1</b>		
<b>Assessment Objective</b>		
<p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization maintains visitor access records to the facility where the information system resides <i>for one (1) year</i>;</li> <li>(ii) the organization reviews the visitor access records in accordance with the organization-defined frequency.</li> </ul>		
<b>Assessment Methods And Objects</b>		
<p><b>Examine:</b> Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; other relevant documents or records.</p>		
<b>PE-12 – Emergency Lighting (Low)</b>		<b>P1</b>
<b>Control</b>		
<p>The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.</p>		
<b>Guidance</b>		
<p><i>This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.</i></p>		

Reference(s): FISCAM: <i>AS-5</i> , CP-2	Related Controls Requirement(s): <i>CP-2</i> , <i>CP-7</i>
<b>ASSESSMENT PROCEDURE: PE-12.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization employs <i>and maintains an</i> automatic emergency lighting for the information system that activates in the event of a power outage or disruption;</li> <li>(ii) the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility;</li> <li>(iii) the organization maintains the automatic emergency lighting for the information system.</li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> 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.</p>	
<b>PE-13 – Fire Protection (Low)</b>	
<p><b>Control</b></p> <p>The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.</p>	
<p><b>Guidance</b></p> <p><i>This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.</i> Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.</p>	
Reference(s): FISCAM: <i>AS-5</i> , CP-2; <i>IRS-1075: 4.3.12#1</i>	Related Controls Requirement(s):
<b>ASSESSMENT PROCEDURE: PE-13.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source;</li> <li>(ii) the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.</li> </ul>	

### Assessment Methods And Objects

**Examine:** Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records.

### PE-14 – Temperature and Humidity Controls (Low)

**PI**

#### Control

The organization:

- a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and
- b. Monitors temperature and humidity levels *within the defined frequency (defined in the applicable security plan).*

#### Implementation Standard(s)

- 1. Evaluate the level of alert and follow prescribed guidelines for that alert level.
- 4. (For CSP only) For service providers, this Standard replaces the above Control. The organization:*
  - a. Maintains temperature and humidity levels within the facility where the information system resides at levels consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments; and*
  - b. Monitors temperature and humidity levels continuously.*
- 5. (For CSP only) For service providers, the organization measures temperature at server inlets and humidity levels by dew point.*

#### Guidance

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

**Reference(s):** FISCAM: *AS-5*, CP-2

**Related Controls Requirement(s):** *AT-3*

### ASSESSMENT PROCEDURE: PE-14.1

#### Assessment Objective

Determine if:

- (i)* the organization defines the acceptable temperature and humidity levels within the facility where the information system resides;
- (ii)* the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels;
- (iii)* the organization defines the frequency to monitor temperature and humidity levels;

(iv) the organization monitors the temperature and humidity levels within the defined frequency (*defined in the applicable security plan*).

(v) the organization meets all the requirements specified in the applicable Implementation Standard(s).

#### Assessment Methods And Objects

**Examine:** Physical and environmental protection policy; procedures addressing temperature and humidity control; security plan; temperature and humidity controls; facility housing the information system; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records.

#### PE-15 – Water Damage Protection (Low)

**P1**

#### Control

The organization protects the information system from damage resulting from water leakage by providing master shutoff *or isolation* valves that are accessible, working properly, and known to key personnel.

#### Guidance

*This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.*

**Reference(s):** FISCAM: *AS-5*, CP-2

**Related Controls Requirement(s):** *AT-3*

#### ASSESSMENT PROCEDURE: PE-15.1

#### Assessment Objective

Determine if:

(i) the organization protects the information system from damage resulting from water leakage by providing master shutoff *or isolation* 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 valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; other relevant documents or records.

#### PE-16 – Delivery and Removal (Low)

**P2**

#### Control

*The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the*



*facility and maintains records of those items.*

**Implementation Standard(s)**

*1. (For CSP only) For service providers, this Standard replaces the above Control. The organization authorizes, monitors, and controls the flow of all information system components entering and exiting the facility and maintains records of those items.*

**Guidance**

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

**Reference(s):** FISCAM: AC-6, *AS-2*; *IRS-1075: 4.3.2#11*

**Related Controls Requirement(s):** *CM-3, MA-2, MA-3, MP-5, SA-12*

**ASSESSMENT PROCEDURE: PE-16.1**

**Assessment Objective**

Determine if:

- (i)* the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility;
- (ii)* the organization maintains records of information system components entering and exiting the facility.

**Assessment Methods And Objects**

**Examine:** Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; security plan; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records.

## 12.0 PLANNING (PL)

*Error! Reference source not found.*

PL-1 – Security Planning Policy and Procedures (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li>1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; <i>and</i></li> </ol> <p><i>b. Reviews and updates (as necessary) the current:</i></p> <ol style="list-style-type: none"> <li>1. Security planning policy within every three hundred sixty-five (365) days; and</li> <li>2. Security planning procedures within every three hundred sixty-five (365) days.</li> </ol>		
<b>Guidance</b> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>PL</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. <i>The policy</i> can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing</i> policy <i>and procedures</i>.</p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: <i>9.13#1.1-2; NIST SP: 800-12, 800-18, 800-100</i>		<b>Related Controls Requirement(s):</b> <i>PM-9</i>
<b>ASSESSMENT PROCEDURE: PL-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <p><i>(i)</i> the organization develops and documents security planning policy;</p> <p><i>(ii)</i> the organization security planning policy addresses:</p> <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> <li>- roles and responsibilities;</li> </ul>		

- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented security planning policy to *applicable personnel* within the organization having associated security planning roles and responsibilities;

(iv) the organization develops and documents security planning procedures;

(v) the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls;

(vi) the organization disseminates documented security planning procedures to *applicable personnel* within the organization having associated security planning roles and responsibilities;

(vii) the organization reviews *and* updates the security planning policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

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

#### PL-2 – System Security Plan (Low)

*Assurance - PI*

#### Control

The organization:

a. Develops a security plan for the information system that is consistent with the *Risk Management Handbook (RMH) Procedures; and*

1. Is consistent with the organization's enterprise architecture;

2. Explicitly defines the authorization boundary for the system;

3. Describes the operational context of the information system in terms of missions and business processes;

4. Provides the security categorization of the information system including supporting rationale;

5. Describes the operational environment for the information system *and* relationships with or connections to other information systems;

6. Provides an overview of the security requirements for the system;

7. *Identifies any relevant overlays, if applicable;*

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. *Distributes copies of the security plan and communicates subsequent changes to the plan to stakeholders;*

- c.* Reviews the security plan for the information system within every three hundred sixty-five (365) days; and
- d.* Updates the plan, minimally every three (3) years, to address current conditions or whenever:
  - There are significant changes to the information system/environment of operation that affect security;
  - Problems are identified during plan implementation or security control assessments;
  - When the data sensitivity level increases;
  - After a serious security violation due to changes in the threat environment; or
  - Before the previous security authorization expires; *and*
- e. Protects the security plan from unauthorized disclosure and modification.*

#### Guidance

*Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in NIST 800-53 Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). NIST 800-53 Appendix I provides guidance on developing overlays. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.*

All CMS information systems and major applications are covered by a security plan, which is compliant with current CMS procedures.

**Reference(s):** FISCAM: AS-1, SM-1; HIPAA: 164.310(a)(2)(ii), 164.316(a), 164.316(b)(1); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.3#6, 6.3.5#3, 7.1#1, 7.1#2, 7.1#3, 9.13#1.3, 9.18.1#2, 9.18.1#3; NIST SP: 800-18

**Related Controls Requirement(s):** AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-5, PL-7, PM-1, PM-8, PM-9,

	<i>PM-11, SA-5, SA-17</i>
<b>ASSESSMENT PROCEDURE: PL-2.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li><i>(i) the organization develops a security plan for the information system that <b>is consistent with the RMH Procedures</b>:</i> <ul style="list-style-type: none"> <li>- is consistent with the organization's enterprise architecture;</li> <li>- explicitly defines the authorization boundary for the system;</li> <li>- describes the operational context of the information system in terms of mission and business processes;</li> <li>- provides the security categorization of the information system including supporting rationale;</li> <li>- describes the operational environment for the information system <b>and</b> relationships with or connections to other information systems;</li> <li>- provides an overview of the security requirements for the system;</li> <li>- <i>identifies any relevant overlays, if applicable;</i></li> <li>- describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions;</li> <li>- is reviewed and approved by the authorizing official or designated representative prior to plan implementation;</li> </ul> </li> <li><i>(ii) the organization <b>distributes copies of</b> the security plan <b>and communicates subsequent changes to the plan to stakeholders</b>;</i></li> <li><i>(iii) the organization reviews the security plan in accordance with the organization-defined frequency, minimally every three (3) years;</i></li> <li><i>(iv) the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.</i></li> <li><i>(v) the organization protects the security plan from unauthorized disclosure and modification.</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> Security planning policy; procedures addressing <i>security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates</i>; other relevant documents or records.</p>	
<b>PL-4 – Rules of Behavior (Low)</b>	
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;</i></li> </ul>	

- b. Receives an acknowledgment (paper or electronic) from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;*
- c. Reviews and updates the rules of behavior every three hundred sixty-five (365) days; and*
- d. Requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated.*

**Guidance**

*This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures (or other electronic mechanisms) for acknowledging rules of behavior. Rules of behavior are aligned with DHHS requirements posted at <http://hhs.gov/ocio/policy/2008-0001.003s.html>, and made readily available.*

**Reference(s):** FISCAM: AS-1, SM-4; HSPD 7: J(35); IRS-1075: 9.13#1.5; NIST SP: 800-18

**Related Controls Requirement(s):** AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, MP-7, PS-6, PS-8, SA-5

**ASSESSMENT PROCEDURE: PL-4.1**

**Assessment Objective**

- Determine if:*
- (i) the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;*
  - (ii) the organization makes the rules available to individuals requiring access to the information system users, and requires individuals to read and acknowledge the rules of behavior within every three hundred sixty-five (365) days thereafter;*
  - (iii) the organization receives a signed acknowledgement (paper or electronic) from individuals indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;*
  - (iv) the organization requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated.*

***Assessment Methods And Objects***

*Examine: Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records.*

***PL-5 – Privacy Impact Assessment (Low)***

***P0***

***Control***

*[Withdrawn: Incorporated into AR-2].*

### 13.0 PERSONNEL SECURITY (PS)

*Error! Reference source not found.*

PS-1 – Personnel Security Policy and Procedures (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li>1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; <i>and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li>1. Personnel security policy within every three hundred sixty-five (365) days; and</li> <li>2. Personnel security procedures within every three hundred sixty-five (365) days.</li> </ol>		
<b>Guidance</b> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>PS</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing</i> policy <i>and procedures</i>.</p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3, SM-4; <i>HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C); IRS-1075: 9.12#1; NIST SP: 800-12, 800-100</i>		<b>Related Controls Requirement(s):</b> <i>PM-9</i>
<b>ASSESSMENT PROCEDURE: PS-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <p><i>(i)</i> the organization develops and documents personnel security policy;</p> <p><i>(ii)</i> the organization personnel security policy addresses:</p> <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> </ul>		



- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented personnel security policy to *applicable personnel* within the organization having associated personnel security roles and responsibilities;

(iv) the organization develops and documents personnel security procedures;

(v) the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls;

(vi) the organization disseminates documented personnel security procedures to *applicable personnel* within the organization having associated personnel security roles and responsibilities;

(vii) the organization reviews *and* updates the personnel security policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

**Examine:** Personnel security policy and procedures, other relevant documents or records.

#### PS-2 – Position *Risk Designation* (Low)

*PI*

#### Control

The organization:

- a. Assigns a risk designation to all *organizational* positions;
- b. Establishes screening criteria for individuals filling those positions; and
- c. Reviews and revises position risk designations within every three hundred sixty-five (365) days.

#### *Implementation Standard(s)*

*1. (For CSP only) For service providers, the organization reviews and revises position risk designations at least every three (3) years.*

#### Guidance

Position risk designations *reflect* Office of Personnel Management policy and guidance. *Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).*

**Reference(s):** FISCAM: *AS-1, AS-4*, SD-1, SD-2, SM-4; *HIPAA: 164.308(a)(3)(ii)(B)*; IRS-1075: *9.12#2.1*

**Related Controls Requirement(s):** *AT-3, PL-2, PS-3*

## ASSESSMENT PROCEDURE: PS-2.1

### Assessment Objective

Determine if:

- (i) the organization assigns a risk designations to all *organizational* positions;
- (ii) the organization establishes a screening criteria for individuals filling organizational positions;
- (iii) the organization defines in the security plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions;
- (iv) the organization reviews/revises position risk designations within every three hundred sixty-five (365) days.
- (v) *(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

### Assessment Methods And Objects

**Examine:** Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; other relevant documents or records.

## PS-3 – Personnel Screening (Low)

*PI*

### Control

The organization:

- a. Screens individuals prior to authorizing access to the information system;
- b. Rescreens individuals periodically, consistent with the *risk designation* of the position; *and*
- c. *When an employee moves from one position to another, the higher level of clearance should be adjudicated.*

### Implementation Standard(s)

1. Require *that individuals with significant security responsibilities be assigned and hold, at a minimum, a Level 5 Public Trust sensitivity level* clearance as defined in *the HHS Personnel Security/Suitability Handbook. Assign other individuals with Public Trust positions the appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook.*
2. *(For CSP only) For service providers, this Standard replaces the above Control and Standard. The organization rescreens individuals according to following:*
  - (a) *For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance.*
  - (b) *For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions.*

<b>Guidance</b> <i>Personnel</i> screening and rescreening <i>activities reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i> , standards, guidance, and <i>specific</i> criteria established for the risk designations of assigned <i>positions</i> . <i>Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.</i>	
<b>Reference(s):</b> <i>FIPS Pub: 199, 201; FISCAM: AS-1, SM-4; HIPAA: 164.308(a)(3)(ii)(B); IRS-1075: 9.12#2.2; NIST SP: 800-60, 800-73, 800-76, 800-78</i>	<b>Related Controls Requirement(s):</b> <i>AC-2, IA-4, PE-2, PS-2</i>
<b>ASSESSMENT PROCEDURE: PS-3.1</b>	
<b>Assessment Objective</b> Determine if: <i>(i) the organization screens individuals prior to authorizing access to the information system;</i> <i>(ii) the organization rescreens individuals periodically, consistent with the risk designation of the position;</i> <i>(iii) the organization requires that when an employee moves from one position to another, the higher level of clearance should be adjudicated.</i> <i>(iv) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i>	
<b>Assessment Methods And Objects</b> <b>Examine:</b> Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records.	
<b>PS-4 – Personnel Termination (Low)</b>	
<b>Control</b> The organization, upon termination of individual employment: a. <i>Disables information</i> system access <i>in accordance with Implementation Standard 1;</i> b. <i>Terminates/revokes any authenticators/credentials associated with the individual;</i> c. Conducts exit interviews <i>that include a discussion of non-disclosure of information security and privacy information;</i> d. Retrieves all security-related <i>organizational</i> information system-related property; e. Retains access to <i>organizational</i> information and information systems formerly controlled by terminated individual; f. <i>Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day; and</i> g. Immediately escorts employees terminated for cause out of the organization. <b>Implementation Standard(s)</b> 1. System access must be revoked immediately following employee termination.	

*2. All access and privileges to systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence).*

#### Guidance

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

Appropriate personnel have access to official records created by terminated employees that are stored on information systems.

**Reference(s):** FISCAM: *AS-1*, SM-4; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: *9.12#3*

**Related Controls Requirement(s):** *AC-2, IA-4, PE-2, PS-5, PS-6*

#### ASSESSMENT PROCEDURE: PS-4.1

##### Assessment Objective

Determine if:

- (i) the organization, upon termination of individual employment:
  - *disables information system access in accordance with Implementation Standard 1;*
  - *terminates/revokes any authenticators/credentials associated with the individual;*
- (ii) the organization, upon termination of individual employment:
  - *conducts exit interviews that include a discussion of non-disclosure of information security and privacy information;*
- (iii) the organization, upon termination of individual employment:
  - *retrieves all security-related organizational information system-related property;*
  - retains access to *organizational* information and information systems formerly controlled by terminated individual;
- (iv) the organization, upon termination of individual employment:
  - *notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day;*
  - immediately escorts employees terminated for cause out of the organization.
- (v) the organization meets all the requirements specified in the applicable Implementation Standard(s).

## Assessment Methods And Objects

**Examine:** Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.

## PS-5 – Personnel Transfer (Low)

**P2**

### Control

The organization:

*a. Reviews and confirms ongoing operational need for current* logical and physical access authorizations to information systems/facilities when *individuals* are reassigned or transferred to other positions within the organization;

*b. Initiates the following transfer or reassignment actions during the formal transfer process:*

*(i). Re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes);*

*(ii). Notification to security management;*

*(iii). Closing obsolete accounts and establishing new accounts;*

*(iv). When an employee moves to a new position of trust, logical and physical access controls must be re-evaluated as soon as possible but not to exceed thirty (30) days;*

*c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and*

*d. Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day.*

### Implementation Standard(s)

*1. (For CSP only) For service providers, the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates organization-defined transfer or reassignment actions within five (5) days following the formal transfer action.*

*2. (For CSP only) For service providers, the organization defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the JAB.*

### Guidance

This control applies when *reassignments* or transfers of *individuals* are permanent or of such extended durations as to make the actions warranted. *Organizations define* actions appropriate for the types of reassignments or transfers, whether permanent or *extended*. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (*i.e., privileges*); and (iv) providing for access to official records to which *individuals* had access at previous work locations and in previous information system accounts.

<b>Reference(s):</b> FISCAM: <i>AS-1</i> , SM-4; <i>HIPAA: 164.308(a)(3)(ii)(C)</i> ; IRS-1075: <i>9.12#4.1</i>	<b>Related Controls Requirement(s):</b> <i>AC-2, IA-4, PE-2, PS-4</i>
<b>ASSESSMENT PROCEDURE: PS-5.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization reviews <i>and confirms ongoing operational need for current</i> logical and physical access authorizations to information systems/facilities when <i>individuals</i> are reassigned or transferred to other positions within the organization;</li> <li>(ii) the organization <i>initiates</i> the <i>following</i> transfer or reassignment actions <i>during</i> the formal transfer <i>process</i>: <ul style="list-style-type: none"> <li>- <i>re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes);</i></li> <li>- <i>notification to security management;</i></li> <li>- <i>closing obsolete accounts and establishing new accounts;</i></li> <li>- <i>when an employee moves to a new position of trust, logical and physical access controls must be re-evaluated as soon as possible but not to exceed thirty (30) days;</i></li> </ul> </li> <li>(iii) the organization initiates <i>modifies access authorization as needed to correspond with any changes in operational need due to</i> reassignment <i>or transfer</i>;</li> <li>(iv) <i>the organization notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day.</i></li> <li>(v) <i>(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.</p>	
<b>PS-6 – Access Agreements (Low)</b>	
<p style="text-align: right;"><i>Assurance - P3</i></p> <p><b>Control</b></p> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. <i>Develops and documents access agreements for organizational</i> information systems;</li> <li>b. Reviews <i>and</i> updates the access agreements as part of the system security authorization or when a contract is renewed or extended, <i>but minimally within every three hundred sixty-five (365) days, whichever occurs first; and</i></li> <li>c. <i>Ensures that individuals requiring access to organizational information and information systems:</i> <ul style="list-style-type: none"> <li>1. <i>Acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and</i></li> <li>2. <i>Re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated.</i></li> </ul> </li> </ul>	

<b>Guidance</b> <p>Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with <i>organizational</i> information systems to which access is authorized. <i>Organizations can use electronic signatures to acknowledge</i> access agreements unless specifically prohibited by organizational policy.</p>	
<b>Reference(s):</b> FISCAM: AS-1, <i>AS-4</i> , SD-1, SD-2, SM-4; <i>HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(B), 164.310(b), 164.310(d)(2)(iii), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii); IRS-1075: 9.12#4.2</i>	<b>Related Controls Requirement(s):</b> <i>PL-4, PS-2, PS-3, PS-4, PS-8</i>
<b>ASSESSMENT PROCEDURE: PS-6.1</b>	
<b>Assessment Objective</b> <p>Determine if:</p> <ul style="list-style-type: none"> <li><i>(i) the organization identifies appropriate access agreements for individuals requiring access to information and information systems;</i></li> <li><i>(ii) individuals requiring access to organizational information and information systems acknowledge appropriate access agreements prior to being granted access;</i></li> <li><i>(iii) the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates for access agreements;</i></li> <li><i>(iv) the organization reviews and updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first;</i></li> <li><i>(v) the organization ensures that individuals requiring access to organizational information and information systems:</i> <ul style="list-style-type: none"> <li><i>- acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and</i></li> <li><i>- re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated</i></li> </ul> </li> </ul>	
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> Personnel security policy; procedures addressing access agreements for organizational information and information systems; security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records.</p>	
<b>PS-7 – Third-Party Personnel Security (Low)</b>	
<b>Control</b> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;</li> </ul>	



- b. *Requires third-party providers to comply with personnel security policies and procedures established by the organization;*
- c. *Documents personnel security requirements;*
- d. *Requires third-party providers to notify Contracting Officers or Contracting Officer Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days; and*
- e. Monitors provider compliance.

**Implementation Standard(s)**

1. Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.

**Guidance**

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

**Reference(s):** FISCAM: AS-1, SM-4, SM-7; *HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.308(b)(1), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii); IRS-1075: 9.12#4.4; NIST SP: 800-35*

**Related Controls Requirement(s):** *PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21*

**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;
- (ii) the organization *requires third-party providers to comply with personnel security policies and procedures established by the organization, and documents personnel security requirements;*
- (iii) *the organization requires third-party providers to notify Contracting Officers or Contracting Officer Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days; and monitors provider*



*compliance.*

*(iv)* the organization meets all the requirements specified in the applicable Implementation Standard(s).

#### Assessment Methods And Objects

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

#### PS-8 – Personnel Sanctions (Low)

*P3*

#### Control

The organization:

*a.* Employs a formal sanctions process for *individuals* failing to comply with established information security policies and procedures; *and*

*b. Notifies defined personnel or roles (defined in the applicable security plan) within defined a time period (defined in the applicable security plan) when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.*

#### Guidance

*Organizational* sanctions *processes reflect* applicable federal laws, Executive Orders, directives, regulations, *policies*, standards, and guidance. *Sanctions processes are* described in access agreements and can be included as part of general personnel policies and procedures for *organizations*. *Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.*

**Reference(s):** FISCAM: *AS-1*, SM-4; HIPAA: 164.308(a)(1)(ii)(C); *IRS-1075: 9.12#4.3*

**Related Controls Requirement(s):** *PL-4, PS-6*

#### ASSESSMENT PROCEDURE: PS-8.1

#### Assessment Objective

Determine if:

*(i)* the organization employs a formal sanctions process for *individuals* failing to comply with established information security policies and procedures;

*(ii) the organization notifies defined personnel or roles (defined in the applicable security plan) within defined a time period (defined in the applicable security plan) when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.*

#### Assessment Methods And Objects

**Examine:** Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions;

other relevant documents or records.

## 14.0 RISK ASSESSMENT (RA)

*Error! Reference source not found.*

RA-1 – Risk Assessment Policy and Procedures (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls on information systems and paper records; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. Risk assessment policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. Risk assessment procedures within every three hundred sixty-five (365) days.</i></li> </ol>		
<b>Guidance</b> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>RA</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing</i> policy <i>and procedures</i>.</p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(1)(i), 164.316(a); IRS-1075: 9.14#1.1-2; NIST SP: 800-12, 800-30, 800-100		<b>Related Controls Requirement(s):</b> PM-9
<b>ASSESSMENT PROCEDURE: RA-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <p><i>(i) the organization develops and documents risk assessment policy;</i></p> <p><i>(ii) the organization risk assessment policy addresses:</i></p> <ul style="list-style-type: none"> <li><i>- purpose;</i></li> <li><i>- scope;</i></li> </ul>		

- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented risk assessment policy to *applicable personnel* within the organization having associated risk assessment roles and responsibilities;

(iv) the organization develops and documents risk assessment procedures;

(v) the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls *on information systems and paper records*;

(vi) the organization disseminates documented risk assessment procedures to *applicable personnel* within the organization having associated risk assessment roles and responsibilities;

(vii) the organization reviews *and* updates the risk assessment policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

**Examine:** Risk assessment policy and procedures; other relevant documents or records.

#### RA-2 – Security Categorization (Low)

*PI*

#### Control

The organization:

- a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
- c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

#### Guidance

Clearly defined authorization *boundaries are* a prerequisite for effective security categorization *decisions*. Security *categories describe* the potential adverse impacts to *organizational* operations, *organizational* assets, and individuals *if organizational* information and information *systems are* comprised through a loss of confidentiality, integrity, or availability. *Organizations conduct* the security categorization process as an organization-wide activity with the involvement of *chief information officers*, senior information security *officers, information system owners, mission/business owners*, and information owners/stewards. *Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act*

*of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted.*

All CMS information systems categorized as High or Moderate are considered sensitive or to contain sensitive information. All CMS information systems categorized as Low are considered non-sensitive or to contain non-sensitive information. Organizations implement the minimum security requirements and controls as established in the current CMS Information Security ARS Standard, based on the system security categorization.

**Reference(s):** *FIPS Pub: 199; FISCAM: AS-1, SM-2; HIPAA: 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7)(ii)(E); IRS-1075: 4.1#2; NIST SP: 800-30, 800-39, 800-60*

**Related Controls Requirement(s):** *CM-8, MP-4, RA-3, SC-7*

#### ASSESSMENT PROCEDURE: RA-2.1

##### Assessment Objective

Determine if:

- (i) the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;*
- (ii) the organization documents the security categorization results (including supporting rationale) in the security plan for the information system;*
- (iii) the CMS authorizing official or authorizing official designated representative reviews and approves the security categorization decision.*

##### Assessment Methods And Objects

***Examine:** Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records.*

#### RA-3 – Risk Assessment (Low)

*Assurance - P1*

##### Control

*The organization:*

- a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;*
- b. Documents risk assessment results in the applicable security plan;*
- c. Reviews risk assessment results within every three hundred sixty-five (365) days;*
- d. Disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO; and*

*e. Updates the risk assessment before issuing a new ATO package or within every three (3) years, whichever comes first; or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.*

**Implementation Standard(s)**

- 1. (For CSP only) For service providers, the organization documents risk assessment results in the security assessment report.*
- 2. (For CSP only) For service providers, the organization reviews risk assessment results at least every three (3) years or when a significant change occurs.*

**Guidance**

*Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.*

*(For CSP only) Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.*

**Reference(s):** FISCAM: AS-1, SM-2; HIPAA: 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 6.3.3#2, 9.14#1.3; NIST SP: 800-30, 800-39; OMB: M-04-04; Web: idmanagement.gov

**Related Controls Requirement(s):** PM-9, RA-2

**ASSESSMENT PROCEDURE: RA-3.1**

**Assessment Objective**

*Determine if:*

- (i) the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits*

*that includes the likelihood and magnitude of harm, from the unauthorized:*

- access;*
- use;*
- disclosure;*
- disruption;*
- modification; or*
- destruction;*

*(ii) the organization reviews and updates the risk assessment policy and procedures within every three hundred sixty-five (365) days.*

*(iii) the organization reviews risk assessment results within every three hundred sixty-five (365) days;*

*(v) the organization updates the risk assessment before issuing a new ATO package or within every three (3) years, whichever comes first, or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.*

*(vi) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

*(iv) the organization disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO;*

#### **Assessment Methods And Objects**

**Examine:** Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records.

#### **RA-5 – Vulnerability Scanning (Low)**

**Assurance - P1**

#### **Control**

*The organization:*

- a. Scans for vulnerabilities in the information system and hosted applications within every thirty (30) days and when new vulnerabilities potentially affecting the system/applications are identified and reported;*
- b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 
  - 1. Enumerating platforms, software flaws, and improper configurations;*
  - 2. Formatting checklists and test procedures; and*
  - 3. Measuring vulnerability impact;**
- c. Analyzes vulnerability scan reports and results from security control assessments;*
- d. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational*

*assessment of risk; and*

*e. Shares information obtained from the vulnerability scanning process and security control assessments with affected/related stakeholders on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).*

**Implementation Standard(s)**

- 1. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with CMS IS procedures.*
- 2. (For CSP only) For service providers, the organization scans for vulnerabilities in the information system and hosted applications quarterly; and operating system, web application, and database scans (as applicable); and when new vulnerabilities potentially affecting the system/applications are identified and reported;*
- 3. (For CSP only) For service providers, the organization remediates legitimate high-risk vulnerabilities mitigated within thirty (30) days, and moderate risk vulnerabilities mitigated with ninety (90) days.*

**Guidance**

*Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).*

**Reference(s):** FISCAM: AS-1, AS-3, CM-5, SM-5; HSPD 7: F(19), G(24); NIST SP: 800-40, 800-70, 800-115; Web: [cwe.mitre.org](http://cwe.mitre.org), [nvd.nist.gov](http://nvd.nist.gov)

**Related Controls Requirement(s):** CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2



### **ASSESSMENT PROCEDURE: RA-5.1**

#### **Assessment Objective**

*Determine if:*

- (i) the organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined frequency and when new vulnerabilities potentially affecting the system/applications are identified and reported;*
- (ii) the organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process that focus on:
  - enumerating platforms, software flaws, and improper configurations;*
  - formatting checklists and test procedures;*
  - measuring vulnerability impact;**
- (iii) the organization analyzes vulnerability scan reports and results from security control assessments;*
- (iv) the organization remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk;*
- (v) the organization shares information obtained from the vulnerability scanning process and security control assessments with affected/related stakeholders on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).*
- (vi) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

#### **Assessment Methods And Objects**

**Examine:** Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.

## 15.0 SYSTEM AND SERVICES ACQUISITION (SA)

*Error! Reference source not found.*

SA-1 – System and Services Acquisition Policy and Procedures (Low)	Assurance - P1
<p><b>Control</b></p> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. System and services acquisition policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. System and services acquisition procedures within every three hundred sixty-five (365) days.</i></li> </ol>	
<p><b>Guidance</b></p> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>SA</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing policy and procedures</i>.</p>	
<p><b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; IRS-1075: <i>9.15#1.1-2; NIST SP: 800-12, 800-100</i></p>	<p><b>Related Controls Requirement(s):</b> <i>PM-9</i></p>
<p><b>ASSESSMENT PROCEDURE: SA-1.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ol style="list-style-type: none"> <li><i>(i) the organization develops and documents system services and acquisition policy;</i></li> <li><i>(ii) the organization system services and acquisition policy addresses:</i> <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> </ul> </li> </ol>	

- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented system services and acquisition policy to *applicable personnel* within the organization having associated system services and acquisition roles and responsibilities;

(iv) the organization develops and documents system services and acquisition procedures;

(v) the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls;

(vi) the organization disseminates documented system services and acquisition procedures to *applicable personnel* within the organization having associated system services and acquisition roles and responsibilities;

(vii) the organization reviews *and* updates the system services and acquisition policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

**Examine:** System and services acquisition policy and procedures; other relevant documents or records.

#### SA-2 – Allocation of Resources (Low)

*Assurance - P1*

#### Control

The organization:

- a. *Determines* information security requirements for the information system *or information system service* in mission/business process planning;
- b. Determines, documents, and allocates the resources required to protect the information system *or information system service* as part of its capital planning and investment control process;
- c. Includes information security requirements in mission/business case planning, and
- d. Establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security.

#### Guidance

*Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.*

**Reference(s):** FISCAM: *AS-1, AS-3, CM-3, SM-1; NIST SP: 800-65*

**Related Controls Requirement(s):** *PM-3, PM-11*

<b>ASSESSMENT PROCEDURE: SA-2.1</b>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization <i>determines</i> information security requirements for the information system <i>or information system service</i> in mission/business process planning;</li> <li>(ii) the organization determines, documents, and allocates the resources required to protect the information system <i>or information system service</i> as part of its capital planning and investment control process;</li> <li>(iii) the organization establishes a discrete line item for information security in organizational programming and budgeting documentation;</li> <li>(iv) the organization establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security.</li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; organizational programming and budgeting documentation; other relevant documents or records.</p>	
<p><b>SA-3 – <i>System Development</i> Life Cycle (Low)</b></p>	
<p><b>Assurance - PI</b></p>	
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li>a. <i>Manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS eXpedited Life Cycle (XLC) that incorporates information security control considerations;</i></li> <li>b. <i>Defines and documents information security roles and responsibilities throughout the system development life cycle;</i></li> <li>c. <i>Identifies individuals having information system security roles and responsibilities; and</i></li> <li>d. <i>Integrates the organizational information security risk management process into system development life cycle activities.</i></li> </ul>	
<p><b>Guidance</b></p> <p><i>A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security</i></p>	

*requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies.*

**Reference(s):** FISCAM: AS-3, CM-3; *NIST SP: 800-37, 800-64*

**Related Controls Requirement(s):** *AT-3, PM-7, SA-8*

#### **ASSESSMENT PROCEDURE: SA-3.1**

##### **Assessment Objective**

Determine if:

- (i) the organization manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS **eXpedited Life Cycle (XLC)** that incorporates information security control considerations;*
- (ii) the organization defines and documents information security roles and responsibilities throughout the system development life cycle;*
- (iii) the organization identifies individuals having information system security roles and responsibilities.*
- (iv) the organization integrates the organizational information security risk management process into system development life cycle activities.*

##### **Assessment Methods And Objects**

**Examine:** System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; information system development life cycle documentation; other relevant documents or records.

#### **SA-4 – Acquisition Process (Low)**

*Assurance - PI*

##### **Control**

The organization includes the following requirements, *descriptions*, and *criteria*, explicitly or by reference, in *the acquisition contract for the* information system, *system component, or information system service* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, *guidelines, and organizational mission/business needs*:

- a. Security functional requirements;
- b. Security strength requirements;*

- c. Security assurance requirements;*
- d. Security-related documentation requirements;*
- e. Requirements for protecting security-related documentation;*
- f. Description of the information system development environment and environment in which the system is intended to operate; and*
- g. Acceptance criteria.*

**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 *and privacy* policies and standards, define security *and privacy* roles and responsibilities, and receive approval from CMS officials.

**Guidance**

*Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle. Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA. (For CSP only) The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See <http://www.niap-ccevs.org/vpl> or <http://www.commoncriteriaportal.org/products.html>.*

<p><b>Reference(s):</b> <i>FIPS Pub: 140-2; FISCAM: AS-3, CM-3; HIPAA: 164.314(a)(2)(i); NIST SP: 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Web: acquisition.gov/far, fips201ep.cio.gov, niap-ccevs.org</i></p>	<p><b>Related Controls Requirement(s):</b> <i>CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12</i></p>
<p><b>ASSESSMENT PROCEDURE: SA-4.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <p>(i) the organization includes the following requirements, <i>descriptions</i>, and <i>criteria</i>, explicitly or by reference, in <i>the acquisition contract for the</i> information system, <i>system component, or information system service</i> in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, <i>guidelines, and organizational mission/business needs</i>:</p> <ul style="list-style-type: none"> <li>- security functional requirements;</li> <li>- <i>security strength requirements</i>;</li> <li>- <i>security assurance requirements</i>;</li> <li>- security-related documentation requirements;</li> <li>- requirements <i>for protecting security-related documentation</i>;</li> <li>- <i>description of the information system development environment and environment in which the system is intended to operate</i>;</li> <li>- <i>acceptance criteria</i>.</li> </ul> <p>(ii) the organization meets all the requirements specified in the applicable Implementation Standard(s).</p> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for information systems or services; other relevant documents or records.</p>	
<p><b>SA-4(10) - Use of Approved PIV Products – Enhancement (Low)</b></p>	
<p><b>Control</b></p>	
<p><i>The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.</i></p>	
<p><b>Reference(s):</b></p>	<p><b>Related Controls Requirement(s):</b> <i>IA-2, IA-8</i></p>
<p><b>ASSESSMENT PROCEDURE: SA-4(10).1</b></p>	
<p><b>Assessment Objective</b></p> <p><i>Determine if the organization employs only information technology products on the FIPS 201-approved products list for PIV</i></p>	

*capability implemented within organizational information systems.*

**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 (Low)**

**Assurance - P2**

**Control**

The organization:

a. Obtains administrator documentation for the information system, *system component, or information system service* that describes:

1. Secure configuration, installation, and operation of the system, *component, or service*;
2. Effective use and maintenance of security functions/*mechanisms*; and
3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, *system component, or information system service* that describes:

1. User-accessible security functions/*mechanisms* and how to effectively use those security functions/*mechanisms*;
2. Methods for user interaction, which enables individuals to use the system, *component, or service* in a more secure manner; and
3. User responsibilities in maintaining the security of the system, *component, or service*;

c. Documents attempts to obtain information system, *system component, or information system service* documentation when such documentation is either unavailable or nonexistent, *and evaluate whether such documentation is essential for the effective implementation or operation of security controls*;

*d. Protects documentation as required, in accordance with the risk management strategy; and*

*e. Distributes documentation to defined personnel or roles (defined in the applicable security plan).*

**Implementation Standard(s)**

1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.
2. Maintain an updated list of related system operations and security documentation.
3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation.

**Guidance**

*This control helps organizational personnel understand the implementation and operation of security controls associated with information **systems**, system **components**, and information system services. Organizations consider establishing specific measures*



*to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.*

**Reference(s):** FISCAM: AS-3, AS-5, CM-2, CP-2; IRS-1075: 9.15#1.3

**Related Controls Requirement(s):** CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4

#### **ASSESSMENT PROCEDURE: SA-5.1**

##### **Assessment Objective**

Determine if:

*(i) the organization obtains administrator documentation for the information system, system component, or information system service that describes:*

- secure configuration, installation, and operation of the system, component, or service;
- effective use and maintenance of the security functions/mechanisms;
- known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

*(ii) the organization obtains user documentation for the information system, system component, or information system service that describes:*

- user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
- methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner;
- user responsibilities in maintaining the security of the system, component, or service;

*(iii) the organization obtains user documentation for the information system, system component, or information system service that describes:*

- user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
- methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner;
- user responsibilities in maintaining the security of the system, component, or service;

*(iv) the organization:*

- protects documentation as required, in accordance with the risk management strategy;
- distributes documentation to defined personnel or roles (defined in the applicable security plan).

*(v) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

### Assessment Methods And Objects

**Examine:** System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent information system documentation; other relevant documents or records.

### SA-6 – Software Usage Restrictions (Low)

**P0**

#### Control

*[Withdrawn: Incorporated into CM-10 and SI-7].*

### SA-7 – User-Installed Software (Low)

**P0**

#### Control

*[Withdrawn: Incorporated into CM-11 and SI-7].*

### SA-9 – External Information System Services (Low)

**Assurance - P1**

#### Control

The organization:

- a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
- c. *Employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security control compliance by external service providers on an ongoing basis.*

#### Guidance

External information system *services are services* that *are* implemented outside of the authorization boundaries of organizational information *systems. This includes services* that *are* used by, but not a part of, organizational information *systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish* relationships with external service providers in a variety of ways *including*, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for *managing* risks from the use of external information system services remains with authorizing officials. For services external to

*organizations*, a chain of trust requires that *organizations* establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between *organizations* and *the external providers*. *Organizations document the basis for trust relationships so the relationships can be monitored over time*. External information system services documentation includes government, service *providers*, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

**Reference(s):** HIPAA: 164.308(b)(1), 164.308(b)(4), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii); HSPD 7: D(8); IRS-1075: 9.15#1.4; NIST SP: 800-35

**Related Controls Requirement(s):** CA-3, IR-7, PS-7

#### ASSESSMENT PROCEDURE: SA-9.1

##### Assessment Objective

Determine if:

- (i) the organization requires that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- (ii) the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services;
- (iii) the organization *employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security control compliance by external service providers on an ongoing basis*.

##### Assessment Methods And Objects

**Examine:** System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

## 16.0 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

*Error! Reference source not found.*

SC-1 – System and Communications Protection Policy and Procedures (Low)		Assurance - P1
<b>Control</b> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li>1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</li> <li>2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; <i>and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li>1. System and communications protection policy within every three hundred sixty-five (365) days; <i>and</i></li> <li>2. System and communications protection procedures within every three hundred sixty-five (365) days.</li> </ol>		
<b>Guidance</b> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>SC</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing policy and procedures</i>.</p>		
<b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; IRS-1075: <i>9.16#1, 9.16#2; NIST SP: 800-12, 800-100</i>		<b>Related Controls Requirement(s):</b> <i>PM-9</i>
<b>ASSESSMENT PROCEDURE: SC-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <p><i>(i)</i> the organization develops and documents system and communications protection policy;</p> <p><i>(ii)</i> the organization system and communications protection policy addresses:</p> <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> </ul>		

- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented system and communications protection policy to *applicable personnel* within the organization having associated system and communications protection roles and responsibilities;

(iv) the organization develops and documents system and communications protection procedures;

(v) the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls;

(vi) the organization disseminates documented system and communications protection procedures to *applicable personnel* within the organization having associated system and communications protection roles and responsibilities;

(vii) the organization reviews *and* updates the system and communications protection policy and procedures within every three hundred sixty-five (365) days.

#### **Assessment Methods And Objects**

*Examine: System and communications protection policy and procedures; other relevant documents or records.*

#### **SC-5 – Denial of Service Protection (Low)**

**PI**

##### **Control**

*The information system protects against or limits the effects of the types of denial of service attacks defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable security plan):*

- SANS Organization: [www.sans.org/dosstep](http://www.sans.org/dosstep);
- SANS Organization's Roadmap to Defeating DDoS: [www.sans.org/dosstep/roadmap.php](http://www.sans.org/dosstep/roadmap.php); and
- NIST National Vulnerability Database: <http://nvd.nist.gov/home.cfm>.

##### **Implementation Standard(s)**

*1. (For CSP only) For service providers, the organization defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by JAB.*

##### **Guidance**

*A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational*

*networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.*

**Reference(s):** FISCAM: AC-5, AS-2

**Related Controls Requirement(s):** SC-6, SC-7

### **ASSESSMENT PROCEDURE: SC-5.1**

#### **Assessment Objective**

*Determine if:*

- (i) the organization defines in the security plan, explicitly or by reference, the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system;*
- (ii) the information system protects against or limits the effects of the types of denial of service attacks defined in NIST SP 800-61 and the organization-defined websites by employing defined security safeguards (defined in the applicable security plan).*
- (iii) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

#### **Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records.

### **SC-7 – Boundary Protection (Low)**

**PI**

#### **Control**

The information system:

- a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
- b. Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and*
- c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.*

#### **Implementation Standard(s)**

- 1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
- 2. Although not required, it is recommended that stateful inspection hardware and software is utilized.

#### **Guidance**

*Managed interfaces* include, for example, gateways, routers, firewalls, guards, *network-based malicious code analysis and virtualization systems*, or encrypted tunnels *implemented within a* security architecture (e.g., routers protecting firewalls *or*

application gateways residing on protected *subnetworks*). *Subnetworks that are physically or logically separated from internal networks are* referred to as demilitarized *zones or DMZs*. *Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses*. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may *also* include third party-provided access lines and other service elements. *Such* transmission services may represent sources of increased risk despite contract security provisions.

**Reference(s):** *FIPS Pub: 199; FISCAM: AC-1, AS-2; NIST SP: 800-41, 800-77*

**Related Controls Requirement(s):** AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13

#### ASSESSMENT PROCEDURE: SC-7.1

##### Assessment Objective

Determine if:

- (i) the organization defines the external boundary of the information system;
- (ii) the organization defines key internal boundaries of the information system;
- (iii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system;
- (iv) *the information system implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks;*
- (v) *the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.*
- (vi) the organization meets all the requirements specified in the applicable Implementation Standard(s).

##### Assessment Methods And Objects

**Examine:** System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; other relevant documents or records.



<b>SC-12 – Cryptographic Key Establishment and Management (Low)</b>		<b>PI</b>
<b>Control</b> <p>When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system <i>in accordance with defined requirements (defined in, or referenced by, the applicable security plan) for key generation, distribution, storage, access, and destruction.</i></p>		
<b>Guidance</b> <p>Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. <i>Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.</i></p>		
<b>Reference(s):</b> FISCAM: AC-4, AS-2; HIPAA: 164.312(e)(2)(ii); IRS-1075: 9.18.3#1, 9.18.3#2; NIST SP: 800-56, 800-57		<b>Related Controls Requirement(s):</b> SC-13, SC-17
<b>ASSESSMENT PROCEDURE: SC-12.1</b>		
<b>Assessment Objective</b> <p>Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system <i>in accordance with defined requirements (defined in, or referenced by, the applicable security plan) for key generation, distribution, storage, access, and destruction.</i></p>		
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> System and communications protection policy; procedures addressing cryptographic key management and establishment; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.</p>		
<b>SC-13 – Cryptographic Protection (Low)</b>		<b>PI</b>
<b>Control</b> <p><i>When cryptographic mechanisms are used, the information system implements encryption products that have been validated under the Cryptographic Module Validation Program (see <a href="http://csrc.nist.gov/cryptval/">http://csrc.nist.gov/cryptval/</a>) to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.</i></p>		
<b>Guidance</b> <p><i>Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and</i></p>		



*Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).*

**Reference(s):** *FIPS Pub: 140-2; FISCAM: AC-4, AS-2; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 9.16#2, 9.16#8.2-3; Web: [cnss.gov](http://cnss.gov), [csrc.nist.gov/cryptval](http://csrc.nist.gov/cryptval)*

**Related Controls Requirement(s):** AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7

#### ASSESSMENT PROCEDURE: SC-13.1

##### Assessment Objective

Determine if when cryptographic mechanisms are used, the information system implements *encrypted products* that *have been validated under the Cryptographic Module Validation Program (see <http://csrc.nist.gov/cryptval/>) to confirm compliance with FIPS 140-2, in accordance* with applicable laws, Executive Orders, directives, policies, regulations, *and* standards.

##### Assessment Methods And Objects

**Examine:** System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

#### SC-13(1) - *FIPS-Validated Cryptography* – Enhancement (Low)

**P1**

##### Control

*[Withdrawn: Incorporated into SC-13].*

#### SC-14 – Public Access Protections (Low)

**P0**

##### Control

*[Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].*

#### SC-15 – Collaborative Computing Devices (Low)

**P1**

##### Control

The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or

his/her designated representative. *If collaborative computer is* authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system:

- a. Prohibits remote activation of collaborative computing devices; and
- b. Provides an explicit indication of use to users physically present at the devices.

**Implementation Standard(s)**

1. *(For CSP only) For service providers, the information system prohibits remote activation of collaborative computing devices with no exceptions.*
2. *(For CSP only) For service providers, the information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.*

**Guidance**

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

**Reference(s):** FISCAM: AC-3, *AS-2*

**Related Controls Requirement(s):** *AC-21*

**ASSESSMENT PROCEDURE: SC-15.1**

**Assessment Objective**

Determine if:

- (i)* the organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative;
- (ii)* if authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used;
- (iii)* if authorized, the information system prohibits remote activation of collaborative computing devices;
- (iv)* if authorized, the information system provides an explicit indication of use to users physically present at the devices.
- (v) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

<b>SC-20 – Secure Name/Address Resolution Service (Authoritative Source) (Low)</b>		<b>P1</b>
<b>Control</b> <p>The information system:</p> <ul style="list-style-type: none"> <li>a. Provides additional data origin and integrity artifacts along with the authoritative <i>name resolution</i> data the system returns in response to <i>external</i> name/address resolution queries; and</li> <li>b. <i>Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.</i></li> </ul> <p><b>Implementation Standard(s)</b></p> <ul style="list-style-type: none"> <li>1. <i>Recursive lookups are disabled on all publicly accessible domain name system (DNS) servers.</i></li> </ul>		
<b>Guidance</b> <p>This control enables <i>external clients including, for example</i>, remote <i>Internet</i> clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. <i>Information systems that provide name and address resolution services include, for example</i>, domain name system (DNS) <i>servers. Additional artifacts include, for example</i>, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. <i>The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23.</i> Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.</p>		
<b>Reference(s):</b> FISCAM: AC-2, <i>AS-2; NIST SP: 800-81; OMB: M-08-23</i>		<b>Related Controls Requirement(s):</b> <i>AU-10, SC-8, SC-12, SC-13, SC-21, SC-22</i>
<b>ASSESSMENT PROCEDURE: SC-20.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the information system provides additional data origin and integrity artifacts along with the authoritative <i>name resolution</i> data the system returns in response to <i>external</i> name/address resolution queries;</li> <li>(ii) <i>the information system provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.</i></li> <li>(iii) <i>the organization meets all the requirements specified in the applicable Implementation Standard(s).</i></li> </ul>		

**Assessment Methods And Objects**

**Examine:** System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

**SC-20(1) - *Child Subspaces* – Enhancement (Low)**

**PI**

**Control**

*[Withdrawn: Incorporated into SC-20].*

**SC-21 – *Secure Name/Address Resolution Service (Recursive or Caching Resolver)* (Low)**

**PI**

**Control**

*The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.*

**Guidance**

*Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.*

**Reference(s):** FISCAM: AC-2, AS-2; NIST SP: 800-81

**Related Controls Requirement(s):** SC-20, SC-22

**ASSESSMENT PROCEDURE: SC-21.1**

**Assessment Objective**

*Determine if the information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.*

**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.

<b>SC-22 – Architecture and Provisioning for Name/Address Resolution Service (Low)</b>		<b>P1</b>
<b>Control</b>		
<i>The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.</i>		
<b>Guidance</b>		
<i>Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).</i>		
<b>Reference(s):</b> <i>FISCAM: AC-2, AS-2; NIST SP: 800-81</i>		<b>Related Controls Requirement(s):</b> <i>SC-2, SC-20, SC-21, SC-24</i>
<b>ASSESSMENT PROCEDURE: SC-22.1</b>		
<b>Assessment Objective</b>		
Determine if:		
<i>(i) the information systems that collectively provide name/address resolution service for an organization are fault tolerant;</i>		
<i>(ii) the information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.</i>		
<b>Assessment Methods And Objects</b>		
<i><b>Examine:</b> System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records.</i>		
<b>SC-39 – Process Isolation (Low)</b>		<b>Assurance - P1</b>
<b>Control</b>		
<i>The information system maintains a separate execution domain for each executing process.</i>		

<b>Guidance</b> <i>Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.</i>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s):</b> AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3
<b>ASSESSMENT PROCEDURE: SC-39.1</b>	
<b>Assessment Objective</b> <i>Determine if the information system maintains a separate execution domain for each executing process.</i>	
<b>Assessment Methods And Objects</b> <b>Examine:</b> System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; <i>information system architecture; list of information system physical domains (or environments); information system facility diagrams;</i> other relevant documents or records.	
<b>SC-CMS-2 – Website Usage (Low)</b>	
<b>Control</b> Web sites are operated within the restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and HHS directives and instruction.	
<b>Guidance</b> Monitor the CMS and DHHS security programs to determine <i>if</i> there are any modified directives and instruction.	
<b>Reference(s):</b> <i>IRS-1075: 9.18.4#1</i>	<b>Related Controls Requirement(s):</b>
<b>ASSESSMENT PROCEDURE: SC-CMS-2.1</b>	
<b>Assessment Objective</b> Determine if the organization maintains websites within restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and HHS directives and instruction.	

**Assessment Methods And Objects**

**Examine:** CMS web site baseline and change management documentation for appropriate configurations.

## 17.0 SYSTEM AND INFORMATION INTEGRITY (SI)

*Error! Reference source not found.*

SI-1 – System and Information Integrity Policy and Procedures (Low)	Assurance - P1
<p><b>Control</b></p> <p>The organization:</p> <p><i>a. Develops, documents, and disseminates to applicable personnel:</i></p> <ol style="list-style-type: none"> <li><i>1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</i></li> <li><i>2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and</i></li> </ol> <p><i>b. Reviews and updates the current:</i></p> <ol style="list-style-type: none"> <li><i>1. System and information integrity policy within every three hundred sixty-five (365) days; and</i></li> <li><i>2. System and information integrity procedures within every three hundred sixty-five (365) days.</i></li> </ol>	
<p><b>Guidance</b></p> <p>This control <i>addresses</i> the <i>establishment of</i> policy and procedures for the effective implementation of <i>selected</i> security controls and control enhancements in the <i>SI</i> family. Policy and procedures <i>reflect</i> applicable federal laws, Executive Orders, directives, regulations, <i>policies</i>, standards, and guidance. <i>Security program</i> policies and procedures <i>at the organization level</i> may make the need for <i>system</i>-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for <i>organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The</i> procedures can be <i>established</i> for the security program in general and for particular information <i>systems, if needed</i>. The organizational risk management strategy is a key factor in <i>establishing policy and procedures</i>.</p>	
<p><b>Reference(s):</b> FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.312(c)(1); IRS-1075: <i>9.17#1</i>; <i>NIST SP: 800-12, 800-100</i></p>	<p><b>Related Controls Requirement(s):</b> <i>PM-9</i></p>
<p><b>ASSESSMENT PROCEDURE: SI-1.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ol style="list-style-type: none"> <li>the organization develops and documents system and information integrity policy;</li> <li>the organization system and information integrity policy addresses: <ul style="list-style-type: none"> <li>- purpose;</li> <li>- scope;</li> </ul> </li> </ol>	



- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

(iii) the organization disseminates documented system and information integrity policy to *applicable personnel* within the organization having associated system and information integrity roles and responsibilities;

(iv) the organization develops and documents system and information integrity procedures;

(v) the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls;

(vi) the organization disseminates documented system and information integrity procedures to *applicable personnel* within the organization having associated system and information integrity roles and responsibilities.

(vii) the organization reviews *and* updates the system and information integrity policy and procedures within every three hundred sixty-five (365) days.

#### Assessment Methods And Objects

**Examine:** System and information integrity policy and procedures; other relevant documents or records.

#### SI-2 – Flaw Remediation (Low)

*PI*

#### Control

The organization:

- a. Identifies, reports, and corrects information system flaws;
- b. Tests software *and firmware* updates related to flaw remediation for effectiveness and potential side effects before installation;
- c. *Installs security-relevant software and firmware updates as directed in Implementation Standard 1; and*
- d. Incorporates flaw remediation into the organizational configuration management process.

#### Implementation Standard(s)

1. Correct identified *security-related* information system flaws on production equipment within *ten (10) business* days and all others within thirty (30) calendar days.

- (a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and
- (b) Manage the flaw remediation process centrally.

*2. A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO or his/her designated representative (e.g., the system data owner or CMS CISO) if a security patch is not applied to a security-based system or network.*

## Guidance

*Organizations identify* information systems affected by announced software flaws *including* potential vulnerabilities resulting from those flaws, and report this information to designated organizational *personnel* with information security responsibilities. Security-relevant software updates *include, for example*, patches, service packs, and hot fixes. *Organizations also address* flaws discovered during security assessments, continuous monitoring, incident response activities, *and* system error handling. Organizations *take advantage of available* resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in *organizational* information systems. By *incorporating* flaw remediation into *ongoing* configuration management *processes*, required/anticipated remediation actions *can be* tracked and verified. Flaw remediation *actions* that *can be tracked and verified include, for example, determining whether organizations follow* US-CERT guidance and Information Assurance Vulnerability Alerts. *Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.*

**Reference(s):** FISCAM: AS-3, CM-5; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 9.17#1; NIST SP: 800-40, 800-182

**Related Controls Requirement(s):** CA-2, CA-7, CM-3, CM-5, CM-8, IR-4, MA-2, RA-5, SA-10, SA-11, SI-11

## ASSESSMENT PROCEDURE: SI-2.1

### Assessment Objective

Determine if:

- (i) the organization identifies, reports, and corrects information system flaws;
- (ii) the organization tests software *and firmware* updates related to flaw remediation for effectiveness *and potential side effects* before installation;
- (iii) the organization *installs security-relevant* software *and firmware* updates *as directed in Implementation Standard 1*;
- (iv) the organization incorporates flaw remediation into the organizational configuration management process.
- (v) the organization meets all the requirements specified in the applicable Implementation Standard(s).

### Assessment Methods And Objects

**Examine:** System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities

potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

**SI-2(1) - Central Management – Enhancement (Low)**

**P1**

**Control**

*The organization centrally manages the flaw remediation process.*

**Guidance**

*Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.*

**Reference(s):** *IRS-1075: 9.17#1*

**Related Controls Requirement(s):**

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

**Assessment Objective**

Determine if the organization centrally manages the flaw remediation process.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records.

**SI-2(2) - Automated Flaw Remediation Status – Enhancement (Low)**

**P1**

**Control**

The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

**Reference(s):** *IRS-1075: 9.17#1*

**Related Controls Requirement(s):** *CM-6, SI-4*

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

**Assessment Objective**

Determine if:

(i) the organization defines the frequency of employing automated mechanisms to determine the state of information system

components with regard to flaw remediation;

(ii) the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.

### Assessment Methods And Objects

**Examine:** System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records.

### SI-3 – Malicious Code Protection (Low)

*PI*

#### Control

The organization:

- a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
- b. Updates malicious code protection mechanisms whenever new releases are available in accordance with CMS configuration management policy and procedures;
- c. Configures malicious code protection mechanisms to:
  1. Perform *periodic* scans *of the* information system using the frequency specified in Implementation Standard 1, and real-time scans of files from external sources *at endpoint, and/or network entry/exit points*, as the files are downloaded, opened, or executed in accordance with organizational security policy; and
  2. Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and
- d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

#### Implementation Standard(s)

1. Desktop malicious code scanning software is configured to perform critical system file scans once a week.
2. *(For CSP only) For service providers, the organization configures malicious code protection mechanisms to:*
  - *Perform periodic scans of the information system at least weekly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and*
  - *Block or quarantine malicious code, send alert to administrator, send alert to FedRAMP in response to malicious code detection.*

#### Guidance

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, *workstations, notebook computers, and mobile devices*. Malicious code includes, for example, viruses,

worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed *or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including*, for example, *web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies.* A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and *comprehensive* software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect *organizational* missions/business functions. Traditional malicious code protection mechanisms *cannot always* detect such code. In these situations, organizations rely instead on other *safeguards including*, for example, secure coding practices, configuration management and control, *trusted procurement processes*, and monitoring practices to help ensure that software does not perform functions other than *the functions* intended. *Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.*

**Reference(s):** FISCAM: *AS-3*, CM-5; IRS-1075: *9.17#2.1*; *NIST SP: 800-83*

**Related Controls Requirement(s):** *CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7*

#### **ASSESSMENT PROCEDURE: SI-3.1**

##### **Assessment Objective**

Determine if:

- (i)* the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
- (ii)* the organization updates malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1;
- (iii)* the organization configures malicious code protection mechanisms to:
  - perform periodic scans of the information system in accordance with organization-defined frequency;
  - perform real-time scans of files from external sources *at endpoint and/or network entry/exit points*, as the files are downloaded, opened, or executed in accordance with organizational security policy;
  - *block and quarantine malicious code and send alert to administrator* in response to malicious code detection;
- (iv)* the organization addresses the receipt of false positives during malicious code detection and eradication *and* the resulting potential impact on the availability of the information system.

(v) the organization meets all the requirements specified in the applicable Implementation Standard(s).

#### Assessment Methods And Objects

**Examine:** System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

#### SI-3(1) - *Central Management* – Enhancement (Low)

**PI**

#### Control

*The organization centrally manages malicious code protection mechanisms.*

#### **Implementation Standard(s)**

*1. (For CSP only) SI-3(1) is not required at Low level for FedRAMP-authorized service providers.*

#### **Guidance**

*Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls.*

**Reference(s):** *IRS-1075: 9.17#2.1*

**Related Controls Requirement(s):** *AU-2, SI-8*

#### 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) - *Automatic Updates* – Enhancement (Low)

**PI**

#### Control

*The information system automatically updates malicious code protection mechanisms.*

#### **Implementation Standard(s)**

*1. (For CSP only) SI-3(2) is not required at Low level for FedRAMP-authorized service providers.*

<b>Guidance</b> <p>Malicious code protection mechanisms <i>include, for example</i>, signature definitions. <i>Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.</i></p>	
<b>Reference(s):</b> <i>IRS-1075: 9.17#2.1</i>	<b>Related Controls Requirement(s):</b> <i>SI-8</i>
<b>ASSESSMENT PROCEDURE: SI-3(2).1</b>	
<b>Assessment Objective</b> <p>Determine if the information system automatically updates malicious code protection mechanisms.</p>	
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> 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.</p>	
<b>SI-4 – Information System Monitoring (Low)</b>	
<p style="text-align: right;"><i>Assurance - P1</i></p>	
<b>Control</b> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. Monitors the information system <i>to detect</i>: <ul style="list-style-type: none"> <li><i>1. Attacks and indicators of potential attacks</i> in accordance with <i>the current Risk Management Handbook (RMH), Volume II, Procedure 7.2, Incident Handling</i> ; and</li> <li><i>2. Unauthorized local, network, and remote connections;</i></li> </ul> </li> <li>b. Identifies unauthorized use of the information system <i>through defined techniques and methods (defined in the applicable security plan);</i></li> <li>c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;</li> <li>d. <i>Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;</i></li> <li>e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to <i>organizational</i> operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;</li> <li>f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; <i>and</i></li> <li>g. <i>Provides defined information system monitoring information (defined in the applicable security plan) to defined personnel or roles (defined in the applicable security plan) as needed, and at defined frequency (defined in the applicable security plan).</i></li> </ul> <p><b>Implementation Standard(s)</b></p>	



1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.
2. *(For CSP only) SI-4 is not required at Low level for FedRAMP-authorized service providers.*
3. *(For CSP only) SI-4 is not required at Low level for FedRAMP-authorized service providers.*

#### Guidance

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the *information* system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the *information system*. *Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events.* Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, *scanning tools*, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security *can also be included as* monitoring devices. The granularity of *monitoring* information collected is based on *organizational* monitoring objectives and the capability of information systems to support such *objectives*. *Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.*

**Reference(s):** FISCAM: AC-5, *AS-2*; HIPAA: 164.308(a)(1)(ii)(D), *164.308(a)(5)(ii)(B)*; IRS-1075: *9.17#1, 9.17#2.2*; NIST SP: 800-61, 800-83, 800-92, 800-94, 800-137

**Related Controls Requirement(s):** AC-3, *AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7*

#### ASSESSMENT PROCEDURE: SI-4.1

##### Assessment Objective

Determine if:

- (i) the organization monitors the information system to detect attacks and indicators of potential attacks in accordance with the current RMH, Volume II, Procedure 7.2, Incident Handling;*
- (ii) the organization monitors the information system to detect unauthorized local, network, and remote connections;*



- (iii) the organization identifies unauthorized use of the information system through defined techniques and methods (defined in the applicable security plan);*
- (iv) the organization deploys monitoring devices:*
- strategically within the information system to collect organization-determined essential information;
  - at ad hoc locations within the system to track specific types of transactions of interest to the organization;
- (v) the organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;*
- (vi) 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;*
- (vii) the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.*
- (viii) the organization provides defined information system monitoring information (defined in the applicable security plan) to defined personnel or roles (defined in the applicable security plan) as needed, and at defined frequency (defined in the applicable security plan).*
- (ix) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

#### Assessment Methods And Objects

**Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

#### SI-4(1) - System-Wide Intrusion Detection System – Enhancement (Low)

*Assurance - P1*

#### Control

The organization connects and configures individual intrusion detection tools into *an information system-wide* intrusion detection system.

**Reference(s):** *IRS-1075: 9.17#1, 9.17#2.2*

**Related Controls Requirement(s):**

#### ASSESSMENT PROCEDURE: SI-4(1).1

#### Assessment Objective

Determine if the organization connects and configures individual intrusion detection tools into *an information* system-wide intrusion detection system.

### Assessment Methods And Objects

**Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.

### SI-4(5) - *System-Generated Alerts* – Enhancement (Low)

*Assurance - PI*

#### Control

The information system alerts *to defined personnel or roles (defined in the applicable security plan)* when the following indications of compromise or potential compromise occur:

- (a) Presence of malicious code,
- (b) Unauthorized export of information,
- (c) Signaling to an external information system, or
- (d) Potential intrusions.

#### *Implementation Standard(s)*

1. *(For CSP only) SI-4(5) is not required at Low level or FedRAMP-authorized service providers.*

#### Guidance

Alerts may be generated from a variety of sources, *including*, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. *Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers.*

#### Reference(s):

**Related Controls Requirement(s):** *AU-5, PE-6*

### ASSESSMENT PROCEDURE: SI-4(5).1

#### Assessment Objective

*Determine if* the information system provides *alerts to defined personnel or roles (defined in the applicable security plan)* when any of the organization-defined list of compromise or potential compromise indicators occurs.

#### Assessment Methods And Objects

**Examine:** System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

SI-5 – Security Alerts, Advisories, and Directives (Low)	Assurance - P1
<p><b>Control</b></p> <p>The organization:</p> <ol style="list-style-type: none"> <li>Receives information system security alerts, advisories, and directives from <i>defined</i> external organizations (<i>defined in the applicable security plan</i>) on an ongoing basis;</li> <li>Generates internal security alerts, advisories, and directives as deemed necessary;</li> <li>Disseminates security alerts, advisories, and directives to: <i>defined</i> personnel <i>or roles</i> (<i>defined in the applicable security plan</i>); and</li> <li>Implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.</li> </ol> <p><b>Implementation Standard(s)</b></p> <ol style="list-style-type: none"> <li>(For CSP only) For service providers, the organization disseminates security alerts, advisories, and directives to all staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP.</li> <li>(For CSP only) For service providers, the organization defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives. The list also includes designated FedRAMP personnel.</li> </ol>	
<p><b>Guidance</b></p> <p>The United States Computer Emergency Readiness Team (US-CERT) <i>generates security alerts and advisories</i> to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse <i>effects</i> on <i>organizational</i> operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. <i>External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.</i></p>	
<p><b>Reference(s):</b> FISCAM: AS-3, CM-5; <i>HIPAA: 164.308(a)(5)(ii)(A); NIST SP: 800-40</i></p>	<p><b>Related Controls Requirement(s):</b> <i>SI-2</i></p>
<p><b>ASSESSMENT PROCEDURE: SI-5.1</b></p>	
<p><b>Assessment Objective</b></p> <p>Determine if:</p> <ol style="list-style-type: none"> <li>the organization receives information system security alerts, advisories, and directives from <i>defined</i> external organizations (<i>defined in the applicable security plan</i>) on an ongoing basis;</li> <li>the organization generates internal security alerts, advisories, and directives;</li> </ol>	

- (iii) the organization disseminates security alerts, advisories, and directives to *defined* personnel *or roles (defined in the applicable security plan)*;
- (iv) the organization implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.
- (v) *(For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).*

#### Assessment Methods And Objects

**Examine:** System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records.

#### SI-8 – Spam Protection (Low)

**P2**

#### Control

The organization:

- a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
- b. Updates spam protection mechanisms when new releases are available in accordance with *organizational* configuration management policy and procedures.

#### *Implementation Standard(s)*

- 1. *(For CSP only) SI-8 is not required at Low level for FedRAMP-authorized service providers.*

#### Guidance

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, *remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.*

**Reference(s):** FISCAM: *AS-3, CM-5*; HIPAA: 164.308(a)(5)(ii)(B); *NIST SP: 800-45*

**Related Controls Requirement(s):** *AT-2, AT-3, SC-5, SC-7, SI-3*

#### ASSESSMENT PROCEDURE: SI-8.1

#### Assessment Objective

Determine if:

- (i) the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages;
- (ii) the organization updates spam protection mechanisms when new releases are available in accordance with organizational

configuration management policy and procedures.

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

**SI-12 – Information Handling and Retention (Low)**

**P2**

**Control**

The organization handles and retains information within *the information system* and *information* output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**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**

*Information* handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention.

**Reference(s):** FISCAM: BP-3; IRS-1075: 9.17#1, 9.17#3

**Related Controls Requirement(s):** AC-16, AU-5, AU-11, MP-2, MP-4

**ASSESSMENT PROCEDURE: SI-12.1**

**Assessment Objective**

Determine if:

- (i) the organization handles information within *the information system* and *information* output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements;
- (ii) the organization retains information within *the information system* and *information* output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
- (iii) the organization meets all the requirements specified in the applicable Implementation Standard(s).

**Assessment Methods And Objects**

**Examine:** System and information integrity policy; procedures addressing information system output handling and retention;

media protection policy and procedures; information retention records, other relevant documents or records.

## 18.0 PROGRAM MANAGEMENT (PM)

*Error! Reference source not found.*

<i>PM-1 – Information Security Program Plan (Low)</i>	<i>PI</i>
<p><b>Control</b></p> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. Develops and disseminates an organization-wide information security program plan that: <ul style="list-style-type: none"> <li>1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;</li> <li>2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;</li> <li>3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and</li> <li>4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;</li> </ul> </li> <li>b. Reviews the organization-wide information security program plan within every three hundred sixty-five (365) days;</li> <li>c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and</li> <li>d. Protects the information security program plan from unauthorized disclosure and modification.</li> </ul>	
<p><b>Guidance</b></p> <p>Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.</p> <p>The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security</p>	

*program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems.*

**Reference(s):**

**Related Controls Requirement(s): PM-8**

**ASSESSMENT PROCEDURE: PM-1.1**

**Assessment Objective**

*Determine if:*

*(i) the organization develops an information security program plan for the organization that:*

- provides an overview of the requirements for the security program;*
- provides a description of the security program management controls and common controls in place or planned for meeting security program requirements;*
- provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;*
- includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;*
- is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation;*
- (ii) the organization defines the frequency of information security program plan reviews;*
- (iii) the organization reviews the organization-wide information security program plan in accordance with the organization-defined frequency;*
- (iv) the organization revises the plan to address organizational changes and problems identified during plan implementation or security control assessments; and*
- (v) the organization disseminates the most recent information security program plan to appropriate entities in the organization.*



**Assessment Methods And Objects**

**Examine:** Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or records.

**Interview:** Organizational personnel with security planning and plan implementation responsibilities for the information security program.

**PM-2 – Senior Information Security Officer (Low)**

**P1**

**Control**

The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

**Guidance**

The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

**Reference(s):**

**Related Controls Requirement(s):**

**ASSESSMENT PROCEDURE: PM-2.1**

**Assessment Objective**

Determine if:

- (i) organization appoints a senior information security officer to coordinate, develop, implement, and maintain an organization-wide information security program; and
- (ii) organization empowers the senior information security officer with the mission and resources required to coordinate, develop, implement, and maintain an organization-wide information security program.

**Assessment Methods And Objects**

**Examine:** Information security program policy; information security program plan; documentation addressing roles and responsibilities of the senior information security officer position; information security program mission statement; other relevant documents or records.

**Interview:** Organizational person appointed to the senior information security officer position.

<b>PM-3 – Information Security Resources (Low)</b>		<b>P1</b>
<b>Control</b> <i>The organization:</i> <ul style="list-style-type: none"> <li>a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;</li> <li>b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and</li> <li>c. Ensures that information security resources are available for expenditure as planned.</li> </ul>		
<b>Guidance</b> <i>Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process.</i>		
<b>Reference(s):</b> NIST SP: 800-65		<b>Related Controls Requirement(s):</b> PM-4, SA-2
<b>ASSESSMENT PROCEDURE: PM-3.1</b>		
<b>Assessment Objective</b> <i>Determine if:</i> <ul style="list-style-type: none"> <li>(i) the organization includes in its capital planning and investment requests the resources needed to implement the information security program;</li> <li>(ii) the organization documents all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program;</li> <li>(iii) the organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and</li> <li>(iv) the organization makes the required information security resources available for expenditure as planned.</li> </ul>		
<b>Assessment Methods And Objects</b> <b>Examine:</b> Information security program policy; capital planning and investment policy; procedures addressing management and oversight for information security-related aspects of the capital planning and investment control process; capital planning and investment documentation; documentation of exceptions supporting capital planning and investment requests; business cases; Exhibit 300; Exhibit 53; other relevant documents or records. <b>Interview:</b> Organizational personnel managing and overseeing the information security-related aspects of the capital planning and investment control process.		

<b>PM-4 – Plan of Action and Milestones Process (Low)</b>		<b>P1</b>
<b>Control</b> <p><i>The organization:</i></p> <p><i>a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:</i></p> <ol style="list-style-type: none"> <li><i>1. Are developed and maintained;</i></li> <li><i>2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and</i></li> <li><i>3. Are reported in accordance with OMB FISMA reporting requirements.</i></li> </ol> <p><i>b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.</i></p>		
<b>Guidance</b> <p><i>The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.</i></p>		
<b>Reference(s):</b> NIST SP: 800-37; OMB: M-02-01		<b>Related Controls Requirement(s):</b> CA-5
<b>ASSESSMENT PROCEDURE: PM-4.1</b>		
<b>Assessment Objective</b> <p><i>Determine if:</i></p> <p><i>(i) the organization implements a process to maintain plans of action and milestones for the security program and the associated organizational information systems; and</i></p> <p><i>(ii) the organization implements a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.</i></p>		
<b>Assessment Methods And Objects</b> <p><b>Examine:</b> <i>Information security program policy; plan of action and milestones policy; procedures addressing plan of action and milestones process; plan of action and milestones for the security program; plan of action and milestones for organizational information systems; other relevant documents or records.</i></p>		

<i><b>Interview:</b> Organizational personnel with plan of action and milestones development and implementation responsibilities.</i>	
<b>PM-5 – Information System Inventory (Low)</b>	
<b>Control</b>	
<i>The organization develops and maintains an inventory of its information systems.</i>	
<b>Guidance</b>	
<i>This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.</i>	
<b>Reference(s):</b> Web: omb.gov	<b>Related Controls Requirement(s):</b>
<b>ASSESSMENT PROCEDURE: PM-5.1</b>	
<b>Assessment Objective</b>	
<i>Determine if:</i>	
<i>(i) the organization develops an inventory of its information systems; and</i>	
<i>(ii) the organization maintains an inventory of its information systems.</i>	
<b>Assessment Methods And Objects</b>	
<i><b>Examine:</b> Information security program policy; procedures addressing information system inventory development and maintenance; information system inventory records, other relevant documents or records.</i>	
<i><b>Interview:</b> Organizational personnel with information system inventory development and maintenance responsibilities.</i>	
<b>PM-6 – Information Security Measures of Performance (Low)</b>	
<b>Control</b>	
<i>The organization develops, monitors, and reports on the results of information security measures of performance.</i>	
<b>Guidance</b>	
<i>Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.</i>	
<b>Reference(s):</b> NIST SP: 800-55	<b>Related Controls Requirement(s):</b>
<b>ASSESSMENT PROCEDURE: PM-6.1</b>	
<b>Assessment Objective</b>	
<i>Determine if:</i>	

- (i) the organization develops information security measures of performance;*
- (ii) the organization monitors information security measures of performance; and*
- (iii) the organization reports on the results of information security measures of performance.*

**Assessment Methods And Objects**

**Examine:** *Information security program policy; procedures addressing development, monitoring, and reporting of information security performance measures; information security performance metrics; information security performance measures; results of information security performance measures; other relevant documents or records.*

**PM-7 – Enterprise Architecture (Low)**

**PI**

**Control**

*The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.*

**Guidance**

*The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral information security architecture consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system but at the same time, is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.*

**Reference(s):** *NIST SP: 800-39; Web: fsam.gov*

**Related Controls Requirement(s):** *PL-2, PL-8, PM-11, RA-2, SA-3*

**ASSESSMENT PROCEDURE: PM-7.1**

**Assessment Objective**

*Determine if the organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.*

**Assessment Methods And Objects**

***Examine:** Information security program policy; enterprise architecture policy; procedures addressing information security-related aspects of enterprise architecture development; system development life cycle documentation; enterprise architecture documentation; enterprise security architecture documentation; other relevant documents or records.*

**PM-8 – Critical Infrastructure Plan (Low)**

**PI**

**Control**

*The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.*

**Guidance**

*Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.*

**Reference(s):**

**Related Controls Requirement(s):** PM-1, PM-9, PM-11, RA-3

**ASSESSMENT PROCEDURE: PM-8.1**

**Assessment Objective**

*Determine if:*  
*(i) the organization develops and documents a critical infrastructure and key resource protection plan;*  
*(ii) the organization updates the critical infrastructure and key resource protection plan; and*  
*(iii) the organization addresses information security issues in the critical infrastructure and key resource protection plan.*

**Assessment Methods And Objects**

***Examine:** Information security program policy; critical infrastructure protection policy; procedures addressing critical infrastructure plan development and implementation; procedures addressing critical infrastructure plan reviews and updates; records of critical infrastructure plan reviews and updates; other relevant documents or records.*

***Interview:** Organizational personnel with critical infrastructure plan development and implementation responsibilities.*

**PM-9 – Risk Management Strategy (Low)**

**PI**

**Control**

*The organization:*  
*a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations,*

- and the Nation associated with the operation and use of information systems;*  
*b. Implements the risk management strategy consistently across the organization; and*  
*c. Reviews and updates the risk management strategy as required, to address organizational changes.*

**Guidance**

*An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive.*

**Reference(s):** NIST SP: 800-30, 800-39

**Related Controls Requirement(s):** RA-3

**ASSESSMENT PROCEDURE: PM-9.1**

**Assessment Objective**

*Determine if:*

- (i) the organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and*  
*(ii) the organization implements that strategy consistently across the organization.*

**Assessment Methods And Objects**

**Examine:** *Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records.*

**Interview:** *Organizational personnel with risk management strategy development and implementation responsibilities.*

**PM-10 – Security Authorization Process (Low)**

**PI**

**Control**

*The organization:*

- a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;*  
*b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and*  
*c. Fully integrates the security authorization processes into an organization-wide risk management program.*

<b>Guidance</b> <i>Security authorization processes for information systems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.</i>	
<b>Reference(s):</b> NIST SP: 800-37, 800-39	<b>Related Controls Requirement(s):</b> CA-6
<b>ASSESSMENT PROCEDURE: PM-10.1</b>	
<b>Assessment Objective</b> <i>Determine if:</i> <i>(i) the organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;</i> <i>(ii) the organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and</i> <i>(iii) the organization fully integrates the security authorization processes into an organization-wide risk management program.</i>	
<b>Assessment Methods And Objects</b> <b>Examine:</b> <i>Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.</i> <b>Interview:</b> <i>Organizational personnel with security authorization responsibilities for information systems; organizational personnel with risk management responsibilities.</i>	
<b>PM-11 – Mission/Business Process Definition (Low)</b>	
<b>Control</b> <i>The organization:</i> <i>a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and</i> <i>b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.</i>	



<p><b>Guidance</b></p> <p><i>Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure.</i></p>	
<p><b>Reference(s):</b> FIPS Pub: 199; NIST SP: 800-60</p>	<p><b>Related Controls Requirement(s):</b> PM-7, PM-8, RA-2</p>
<p><b>ASSESSMENT PROCEDURE: PM-11.1</b></p>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and</i></li> <li><i>(ii) the organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> <i>Information security program policy; risk management policy; procedures addressing security categorization of organizational information and information systems; organizational mission/business processes; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records.</i></p> <p><b>Interview:</b> <i>Organizational personnel with mission/business process definition responsibilities; organizational personnel with security categorization and risk management responsibilities for the information security program.</i></p>	
<p><b>PM-12 – Insider Threat Program (Low)</b></p>	
<p><b>Control</b></p> <p><i>The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.</i></p>	

**Guidance**

*Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture.*

*Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines.*

**Reference(s):** Executive Order: 13587

**Related Controls Requirement(s):** AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-1, PM-14, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4

**ASSESSMENT PROCEDURE: PM-12.1**

**Assessment Objective**

*Determine if the organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.*

**Assessment Methods And Objects**

**Examine:** Information security program policy; risk management policy; procedures addressing incident handling and response; other relevant documents or records.

***Interview:** Organizational personnel with risk management responsibilities, organizational personnel with incident response responsibilities.*

**PM-13 – Information Security Workforce (Low)**

**PI**

**Control**

*The organization establishes an information security workforce development and improvement program.*

**Guidance**

*Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.*

**Reference(s):**

**Related Controls Requirement(s):** AT-2, AT-3

**ASSESSMENT PROCEDURE: PM-13.1**

**Assessment Objective**

*Determine if the organization establishes an information security workforce development and improvement program.*

**Assessment Methods And Objects**

***Examine:** Information security program policy; security workforce development and improvement program; security workforce development and improvement program procedures; other relevant documents or records.*

***Interview:** Organizational personnel with risk management responsibilities, organizational personnel with security workforce development program responsibilities.*

**PM-14 – Testing, Training, and Monitoring (Low)**

**PI**

**Control**

*The organization:*

*a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities*

*associated with organizational information systems:*

*1. Are developed and maintained; and*

*2. Continue to be executed in a timely manner;*

*b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.*

**Guidance**

*This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.*

**Reference(s):** NIST SP: 800-16, 800-37, 800-53A, 800-137

**Related Controls Requirement(s):** AT-3, CA-7, CP-4, IR-3, SI-4

**ASSESSMENT PROCEDURE: PM-14.1**

**Assessment Objective**

*Determine if:*

*(i) the organization implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:*

*- are developed and maintained;*

*- continue to be executed in a timely manner;*

*(ii) the organization reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.*

**Assessment Methods And Objects**

**Examine:** *Information security program policy; security testing, training, and monitoring process documentation; security testing, training, and monitoring activities procedures; other relevant documents or records.*

**PM-15 – Contacts with Security Groups and Associations (Low)**

**P3**

**Control**

*The organization establishes and institutionalizes contact with selected groups and associations within the security community:*

<p><i>a. To facilitate ongoing security education and training for organizational personnel;</i>  <i>b. To maintain currency with recommended security practices, techniques, and technologies; and</i>  <i>c. To share current security-related information including threats, vulnerabilities, and incidents.</i></p>	
<p><b>Guidance</b></p> <p><i>Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.</i></p>	
<b>Reference(s):</b>	<b>Related Controls Requirement(s): SI-5</b>
<b>ASSESSMENT PROCEDURE: PM-15.1</b>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i>  <i>(i) the organization establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel;</i>  <i>(ii) the organization establishes and institutionalizes contact with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies;</i>  <i>(iii) the organization establishes and institutionalizes contact with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents.</i></p> <p><b>Assessment Methods And Objects</b></p> <p><i><b>Examine:</b> Information security program policy; security testing, training, and monitoring process documentation; security testing, training, and monitoring activities procedures; other relevant documents or records.</i></p>	
<b>PM-16 – Threat Awareness Program (Low)</b>	
<b>Control</b>	
<p><i>The organization implements a threat awareness program that includes a cross-organization information-sharing capability.</i></p>	
<p><b>Guidance</b></p> <p><i>Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have</i></p>	

*found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.*

**Reference(s):**

**Related Controls Requirement(s):** PM-12, PM-16

**ASSESSMENT PROCEDURE: PM-16.1**

**Assessment Objective**

*Determine if the organization implements a threat awareness program that includes a cross-organization information-sharing capability*

**Assessment Methods And Objects**

**Examine:** Information security program policy; threat awareness program policy; threat awareness program procedures; other relevant documents or records.

## 19.0 AUTHORITY AND PURPOSE (AP)

*Error! Reference source not found.*

<b>AP-1 – Authority to Collect (Low)</b>		<b>PI</b>
<b>Control</b>		
<i>The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.</i>		
<b>Guidance</b>		
<i>Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.</i>		
<b>Reference(s):</b> E-Gov: § 208(c); OMB: Circular A-130 Appendix I; Privacy Act: § 552a(e)		<b>Related Controls Requirement(s):</b> AR-2, DM-1, TR-1, TR-2
<b>ASSESSMENT PROCEDURE: AP-1.1</b>		
<b>Assessment Objective</b>		
<i>Determine if:</i>		
<i>(i) the organization determines the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.</i>		
<i>(ii) the organization documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.</i>		
<b>Assessment Methods And Objects</b>		
<b>Examine:</b> TBD		
<b>Interview:</b> TBD		
<b>ASSESSMENT PROCEDURE: AP-1.1</b>		
<b>Assessment Objective</b>		
<i>Determine if:</i>		

- (i) the organization determines the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.
- (ii) the organization documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

**Assessment Methods And Objects**

**Examine:** Legal authority that permits the collection, use, maintenance, and sharing of PII; PII collection, use, maintenance, and sharing program policy; PII collection, use, maintenance, and sharing program procedures; other relevant documents or records.

**AP-2 – Purpose Specification (Low)**

**P1**

**Control**

The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

**Guidance**

Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.

**Reference(s):** E-Gov: § 208(b), § 208(c); Privacy Act: § 552a(e)(3)(A)-(B)

**Related Controls Requirement(s):** AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2

**ASSESSMENT PROCEDURE: AP-2.1**

**Assessment Objective**

Determine if the organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

**Assessment Methods And Objects**

**Examine:** TBD

**Interview:** TBD



**ASSESSMENT PROCEDURE: AP-2.1**

**Assessment Objective**

*Determine if the organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.*

**Assessment Methods And Objects**

***Examine:** Privacy notice that describes the purpose for which PII can be collected, used, maintained, and shared; other relevant documents or records.*

## 20.0 ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (AR)

*Error! Reference source not found.*

<i>AR-I – Governance and Privacy Program (Low)</i>	<i>PI</i>
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;</i></li> <li><i>b. Monitors federal privacy laws and policy for changes that affect the privacy program;</i></li> <li><i>c. Allocates an appropriate allocation of budget and staffing to implement and operate the organization-wide privacy program;</i></li> <li><i>d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;</i></li> <li><i>e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and</i></li> <li><i>f. Updates privacy plan, policies, and procedures, as required to address changing requirements, but at least biennially.</i></li> </ul>	
<p><b>Guidance</b></p> <p><i>The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.</i></p> <p><i>To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy</i></p>	

*controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.*

**Reference(s):** 44 U.S.C.: § 3541; OMB: Circular A-130, M-03-22, M-05-08, M-07-16; Privacy Act: § 552a

**Related Controls Requirement(s):**

### **ASSESSMENT PROCEDURE: AR-1.1**

#### **Assessment Objective**

*Determine if:*

- (i) the organization appoints a SAOP/CPO accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;*
- (ii) the organization monitors federal privacy laws and policy for changes that affect the privacy program;*
- (iii) the organization allocates an appropriate allocation of budget and staffing to implement and operate the organization-wide privacy program;*
- (iv) the organization develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;*
- (v) the organization develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII;*
- (vi) the organization updates privacy plan, policies, and procedures, as required to address changing requirements, but at least biennially.*

#### **Assessment Methods And Objects**

**Examine:** *Organizational governance and privacy policy; governance and privacy program plan; governance and privacy procedures; budget and staffing documentation; strategic organizational privacy plan; privacy policies and procedures; information system privacy and security controls; other relevant documents or records.*

### **AR-2 – Privacy Impact and Risk Assessment (Low)**

**PI**

#### **Control**

*The organization:*

- a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and*

*b. Conducts Privacy Impact Assessments (PIA) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.*

**Guidance**

*Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.*

**Reference(s):** 44 U.S.C.: § 3541; E-Gov: § 208; OMB: M-03-22, M-05-08, M-10-23

**Related Controls Requirement(s):**

**ASSESSMENT PROCEDURE: AR-2.1**

**Assessment Objective**

*Determine if:*

*(i) the organization documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII;*

*(ii) the organization conducts PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.*

**Assessment Methods And Objects**

**Examine:** *Privacy risk management planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records.*

**AR-3 – Privacy Requirements for Contractors and Service Providers (Low)**

**PI**

**Control**

*The organization:*

- a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and*
- b. Includes privacy requirements in contracts and other acquisition-related documents.*

<b>Guidance</b> <i>Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.</i>	
<b>Reference(s):</b> FAR: Part 24; OMB: Circular A-130; Privacy Act: § 552a(m)	<b>Related Controls Requirement(s):</b> AR-1, AR-5, SA-4
<b>ASSESSMENT PROCEDURE: AR-3.1</b>	
<b>Assessment Objective</b> <i>Determine if:</i> <i>(i) the organization establishes privacy roles, responsibilities, and access requirements for contractors and service providers;</i> <i>(ii) the organization includes privacy requirements in contracts and other acquisition-related documents.</i>	
<b>Assessment Methods And Objects</b> <b>Examine:</b> <i>Organization privacy policy establishing privacy roles, responsibilities, and access requirements for contractors and service providers; privacy requirements in contracts and other acquisition-related documents; other relevant documents or records.</i>	
<b>AR-4 – Privacy Monitoring and Auditing (Low)</b>	
<b>Control</b> <i>The organization monitors and audits privacy controls and internal privacy policy as required to ensure effective implementation.</i>	
<b>Guidance</b> <i>To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in [800-53 Appendix J], organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s). Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to</i>	

*ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials.*

**Reference(s):** 44 U.S.C.: § 3541; E-Gov: § 208; OMB: Circular A-130, M-03-22, M-05-08, M-06-16, M-07-16; Privacy Act: § 552a

**Related Controls Requirement(s):** AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2

#### **ASSESSMENT PROCEDURE: AR-4.1**

##### **Assessment Objective**

*Determine if the organization monitors and audits privacy controls and internal privacy policy as required to ensure effective implementation.*

##### **Assessment Methods And Objects**

**Examine:** Organization privacy policy monitoring and auditing requirements; internal privacy policy to ensure effective privacy control implementation; procedures for monitoring and auditing privacy controls; audit controls and records; other relevant documents or records.

#### **AR-5 – Privacy Awareness and Training (Low)**

**PI**

##### **Control**

*The organization:*

- a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;*
- b. Administers basic privacy training at within every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII within every three hundred sixty-five (365) days; and*
- c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements within every three hundred sixty-five (365) days.*

##### **Guidance**

*Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use*

*requirements identified in public notices, such as Privacy Impact Assessments (PIA) or System of Records Notices (SORN) for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training.*

**Reference(s):** E-Gov: § 208; OMB: M-03-22, M-07-16; Privacy Act: § 552a(e)

**Related Controls Requirement(s):** AR-3, AT-2, AT-3, TR-1

#### **ASSESSMENT PROCEDURE: AR-5.1**

##### **Assessment Objective**

*Determine if:*

- (i) the organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;*
- (ii) the organization administers basic privacy training at within every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII within every three hundred sixty-five (365) days;*
- (iii) the organization ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements within every three hundred sixty-five (365) days.*

##### **Assessment Methods And Objects**

**Examine:** Training and awareness policy; training and awareness program plan strategy; privacy and awareness training material, training records; other relevant documents or records.

#### **ASSESSMENT PROCEDURE: AR-5.1**

##### **Assessment Objective**

*Determine if:*

- (i) the organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;*
- (ii) the organization administers basic privacy training at within every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII within every three hundred sixty-five (365) days;*

*(iii) the organization ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements within every three hundred sixty-five (365) days.*

**Assessment Methods And Objects**

*Examine: Training and awareness policy; training and awareness program plan strategy; privacy and awareness training material, training records; other relevant documents or records.*

**AR-6 – Privacy Reporting (Low)**

**PI**

**Control**

*The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.*

**Guidance**

*Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Agency Official for Privacy (SAOP) reports to OMB; (ii) reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; or (iii) other public reports required by specific statutory mandates or internal policies of organizations. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.*

**Reference(s):** 44 U.S.C.: § 3541; 9/11 Comm Act: § 2000ee-1, Section 803, § 2000ee-3, Section 804; Consol Approp Act: § 522; E-Gov: § 208; OMB: Circular A-130; Privacy Act: § 552a

**Related Controls Requirement(s):**

**ASSESSMENT PROCEDURE: AR-6.1**

**Assessment Objective**

*Determine if:*

- (i) the organization develops privacy reports to the OMB, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance;*
- (ii) the organization disseminates privacy reports to the OMB, Congress, and other oversight bodies, as appropriate, and to senior*



*management and other personnel with responsibility for monitoring privacy program progress and compliance;*  
*(iii) the organization updates privacy reports within the time period specified by specific statutory and regulatory privacy program mandates but no less than within every three hundred sixty-five (365) days.*

**Assessment Methods And Objects**

*Examine: Reports to OMB, Congress, and other oversight bodies, as appropriate; reports to senior management and personnel with responsibility for monitoring privacy program progress and compliance; other relevant documents or records.*

**AR-7 – Privacy-Enhanced System Design and Development (Low)**

**PI**

**Control**

*The organization designs information systems to support privacy by automating privacy controls.*

**Guidance**

*To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization's privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes.*

**Reference(s):** E-Gov: § 208(b), § 208(c); OMB: M-03-22; Privacy Act: § 552a(e)(10)

**Related Controls Requirement(s):** AC-6, AR-4, AR-5, DM-2, TR-1

**ASSESSMENT PROCEDURE: AR-7.1**

**Assessment Objective**

*Determine if the organization designs information systems to support privacy by automating privacy controls.*

**Assessment Methods And Objects**

*Examine: Information system design documentation; other relevant documents or records.*

**AR-8 – Accounting of Disclosures (Low)**

**PI**

**Control**

*The organization:*

*a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:*

- (1) Date, nature, and purpose of each disclosure of a record; and*  
*(2) Name and address of the person or agency to which the disclosure was made;*  
*b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and*  
*c. Makes the accounting of disclosures available to the person named in the record upon request.*

**Guidance**

*The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals.*

**Reference(s):** Privacy Act: § 552a(c)(1), § 552a(c)(3), § 552a(j), § 552a(k)

**Related Controls Requirement(s):** IP-2

**ASSESSMENT PROCEDURE: AR-8.1**

**Assessment Objective**

*Determine if:*

- (i) the organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including:*  
*(ii) the organization retains the accounting of disclosures for the life of the record or five (5) years after the disclosure is made, whichever is longer;*  
*(iii) the organization makes the accounting of disclosures available to the person named in the record upon request.*

**Assessment Methods And Objects**

**Examine:** *Records documenting the disclosures of information held in each system of records under its control; retention policy for the disclosure records; policy for making the disclosures available to the person named in the record upon request; other relevant documents or records.*

## 21.0 DATA QUALITY AND INTEGRITY (DI)

*Error! Reference source not found.*

<b>DI-1 – Data Quality (Low)</b>		<b>PI</b>
<b>Control</b> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;</li> <li>b. Collects PII directly from the individual to the greatest extent practicable;</li> <li>c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the Data Integrity Board; and</li> <li>d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.</li> </ul>		
<b>Guidance</b> <p>Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.</p> <p>When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.</p>		
<b>Reference(s):</b> OMB: M-07-16; Privacy Act: § 552a(c), § 552a(e)		<b>Related Controls Requirement(s):</b> AP-2, DI-2, DM-1, IP-3, SI-10
<b>ASSESSMENT PROCEDURE: DI-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;</li> </ul>		

- (ii) the organization collects PII directly from the individual to the greatest extent practicable;*
- (iii) the organization checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the Data Integrity Board;*
- (iv) the organization issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.*

**Assessment Methods And Objects**

***Examine:** Organization privacy policy; privacy program plan; privacy program procedures; guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information; other relevant documents or records.*

**DI-2 – Data Integrity and Data Integrity Board (Low)**

**P1**

**Control**

*The organization:*

- a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and*
- b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.*

**Guidance**

*Organizations conducting or participating in Computer Matching Agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO). The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under Computer Matching Agreements.*

**Reference(s):** OMB: Circular A-130 Appendix I; Privacy Act: § 552a(a)(8)(A), § 552a(o), § 552a(p), § 552a(u)

**Related Controls Requirement(s):** AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2

**ASSESSMENT PROCEDURE: DI-2.1**

**Assessment Objective**

*Determine if:*

- (i) the organization documents processes to ensure the integrity of PII through existing security controls;*
- (ii) the organization establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching*

*Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.*

***Assessment Methods And Objects***

***Examine:*** *Organization PII integrity policy; PII integrity program plan; PII integrity process and procedures; information system security plan; other relevant documents or records.*

## 22.0 DATA MINIMIZATION AND RETENTION (DM)

*Error! Reference source not found.*

<b>DM-1 – Minimization of Personally Identifiable Information (Low)</b>	<b>PI</b>
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;</i></li> <li><i>b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and</i></li> <li><i>c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, within every three hundred sixty-five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.</i></li> </ul> <p><b>Guidance</b></p> <p><i>Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.</i></p> <p><i>Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules.</i></p> <p><i>By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice.</i></p>	
<p><b>Reference(s):</b> E-Gov: § 208(b); OMB: M-03-22, M-07-16; Privacy Act: § 552a(e)</p>	<p><b>Related Controls Requirement(s):</b> AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1</p>

**ASSESSMENT PROCEDURE: DM-1.1**

**Assessment Objective**

*Determine if:*

- (i) the organization identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;*
- (ii) the organization limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent;*
- (iii) the organization conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, within every three hundred sixty-five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.*

**Assessment Methods And Objects**

***Examine:** Organization privacy data minimization and retention policy; privacy data minimization and retention program plan; privacy data minimization and retention program procedures; PII holding evaluation and review documentation; other relevant documents or records.*

**DM-2 – Data Retention and Disposal (Low)**

**PI**

**Control**

*The organization:*

- a. Retains each collection of personally identifiable information (PII) for minimum allowable necessary to fulfill the purpose(s) identified in the notice or as required by law;*
- b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and*
- c. Uses legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).*

**Guidance**

*NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.*

*Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA*

<p><i>approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII.</i></p> <p><i>Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche may not permit the removal of individual records without the destruction of the entire database contained on such media.</i></p>	
<p><b>Reference(s):</b> 44 U.S.C.: Chapter 29, Chapter 31, Chapter 33; E-Gov: § 208(e); NIST SP: 800-88; OMB: Circular A-130, M-07-16; Privacy Act: § 552a(c)(2), § 552a(e)(1)</p>	<p><b>Related Controls Requirement(s):</b> AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1</p>
<p><b>ASSESSMENT PROCEDURE: DM-2.1</b></p>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization retains each collection of PII for minimum allowable necessary to fulfill the purpose(s) identified in the notice or as required by law;</i></li> <li><i>(ii) the organization disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access;</i></li> <li><i>(iii) the organization uses legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> <i>Organization PII retention policy; PII retention procedures; organization PII disposal policy; PII disposal procedures; other relevant documents or records.</i></p>	
<p><b>DM-3 – Minimization of PII Used in Testing, Training, and Research (Low)</b></p>	
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and</i></li> <li><i>b. Implements controls to protect PII used for testing, training, and research.</i></li> </ul>	
<p><b>Guidance</b></p> <p><i>Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the SAOP/CPO and legal counsel to ensure</i></p>	



<i>that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.</i>	
<b>Reference(s):</b> NIST SP: 800-122	<b>Related Controls Requirement(s):</b>
<b>ASSESSMENT PROCEDURE: DM-3.1</b>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research;</i></li> <li><i>(ii) the organization implements controls to protect PII used for testing, training, and research.</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><i><b>Examine:</b> Organization policies concerning the use of PII used for testing, training, and research; procedures concerning the use of PII used for testing, training, and research; controls used to protect PII used for testing, training, and research; other relevant documents or records.</i></p>	

## 23.0 INDIVIDUAL PARTICIPATION AND REDRESS (IP)

*Error! Reference source not found.*

<i>IP-1 – Consent (Low)</i>	<i>PI</i>
<p><b>Control</b></p> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;</li> <li>b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;</li> <li>c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and</li> <li>d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.</li> </ul>	
<p><b>Guidance</b></p> <p>Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.</p> <p>Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. For example, the Federal Trade Commission’s Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals’ behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization.</p>	

<p><b>Reference(s):</b> E-Gov: § 208(c); OMB: M-03-22, M-10-22; Privacy Act: § 552a(b), § 552a(e)(3)</p>	<p><b>Related Controls Requirement(s):</b> AC-2, AP-1, TR-1, TR-2</p>
<p><b>ASSESSMENT PROCEDURE: IP-1.1</b></p>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;</i></li> <li><i>(ii) the organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;</i></li> <li><i>(iii) the organization obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII;</i></li> <li><i>(iv) the organization ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><i><b>Examine:</b> Organization policy that authorizes the collection, use, maintaining, and sharing of PII prior to its collection; procedures to authorize the collection, use, maintaining, and sharing of PII prior to its collection; other relevant documents or records.</i></p>	
<p><b>IP-2 – Individual Access (Low)</b></p>	
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;</i></li> <li><i>b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;</i></li> <li><i>c. Publishes access procedures in System of Records Notices (SORNs); and</i></li> <li><i>d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.</i></li> </ul>	
<p><b>Guidance</b></p> <p><i>Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer</i></p>	

<i>(CPO) is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding.</i>	
<b>Reference(s):</b> OMB: Circular A-130; Privacy Act: § 552a(c)(3), § 552a(d)(5), § 552a(e)(4), § 552a(j), § 552a(k), § 552a(t)	<b>Related Controls Requirement(s):</b> AR-8, IP-3, TR-1, TR-2
<b>ASSESSMENT PROCEDURE: IP-2.1</b>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i></p> <ul style="list-style-type: none"> <li><i>(i) the organization provides individuals the ability to have access to their PII maintained in its system(s) of records;</i></li> <li><i>(ii) the organization publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;</i></li> <li><i>(iii) the organization publishes access procedures in SORNs;</i></li> <li><i>(iv) the organization adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.</i></li> </ul> <p><b>Assessment Methods And Objects</b></p> <p><b>Examine:</b> <i>Organization policy providing individuals access to their PII maintained in system(s) of records; procedures providing individuals access to their PII maintained in system(s) of record; rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; access procedures in SORNs; other relevant documents or records.</i></p>	
<b>IP-3 – Redress (Low)</b>	
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and</i></li> <li><i>b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.</i></li> </ul>	
<p><b>Guidance</b></p> <p><i>Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes</i></p>	

*demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate. To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information. Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information.*

**Reference(s):** OMB: Circular A-130; Privacy Act: § 552a(c)(4), § 552a(d)

**Related Controls Requirement(s):** IP-2, TR-1, TR-2, UL-2

### **ASSESSMENT PROCEDURE: IP-3.1**

#### **Assessment Objective**

*Determine if:*

- (i) the organization provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate;*
- (ii) the organization establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.*

#### **Assessment Methods And Objects**

**Examine:** *Process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; process for disseminating corrections or amendments of the PII to other authorized users of the PII; process for notifying affected individuals that their information has been corrected or amended; other relevant documents or records.*

### **IP-4 – Complaint Management (Low)**

**PI**

#### **Control**

*The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about*

*the organizational privacy practices.*

**Guidance**

*Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.*

**Reference(s):** OMB: Circular A-130, M-07-16, M-08-09

**Related Controls Requirement(s):** AR-6, IP-3

**ASSESSMENT PROCEDURE: IP-4.1**

**Assessment Objective**

*Determine if the organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.*

**Assessment Methods And Objects**

**Examine:** *Process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices; other relevant documents or records.*

## 24.0 SECURITY (SE)

*Error! Reference source not found.*

<b>SE-1 – Inventory of Personally Identifiable Information (Low)</b>		<b>PI</b>
<b>Control</b> <p>The organization:</p> <ul style="list-style-type: none"> <li>a. Establishes, maintains, and updates, within every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and</li> <li>b. Provides each update of the PII inventory to the Senior Official for Privacy and the Chief information Security Officer to support the establishment of information security requirements for all new or modified information systems containing PII.</li> </ul>		
<b>Guidance</b> <p>The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with NIST 800-53 Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, organizations may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII.</p>		
<b>Reference(s):</b> E-Gov: § 208(b)(2); FIPS Pub: 199; NIST SP: 800-37, 800-122; OMB: Circular A-130 Appendix I, M-03-22; Privacy Act: § 552a(e)(10)		<b>Related Controls Requirement(s):</b> AR-1, AR-4, AR-5, AT-1, DM-1, PM-5
<b>ASSESSMENT PROCEDURE: SE-1.1</b>		
<b>Assessment Objective</b> <p>Determine if:</p> <ul style="list-style-type: none"> <li>(i) the organization establishes, maintains, and updates, within every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII;</li> <li>(ii) the organization provides each update of the PII inventory to the Senior Official for Privacy and the Chief information Security Officer to support the establishment of information security requirements for all new or modified information systems containing PII.</li> </ul>		

**Assessment Methods And Objects**

***Examine:** Organization policy for establishing, maintaining, and updating an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII; inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII; other relevant documents or records.*

**SE-2 – Privacy Incident Response (Low)**

**PI**

**Control**

*The organization:*

- a. Develops and implements a Privacy Incident Response Plan; and*
- b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.*

**Guidance**

*In contrast to the Incident Response (IR) family in NIST 800-53 Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the SAOP/CPO. The plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), consistent with organizational incident management structures; and (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach. Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate.*

**Reference(s):** NIST SP: 800-37; OMB: M-06-19, M-07-16; Privacy Act: § 552a(e), § 552a(i)(1), § 552a(m)

**Related Controls Requirement(s):** AR-1, AR-4, AR-5, AR-6, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-13, AU-14, IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, RA-1



***ASSESSMENT PROCEDURE: SE-2.1***

***Assessment Objective***

*Determine if:*

- (i) the organization develops and implements a Privacy Incident Response Plan;*
- (ii) the organization provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.*

***Assessment Methods And Objects***

***Examine:*** *Organization Privacy Incident Response Plan; privacy incident response procedures; other relevant documents or records.*

## 25.0 TRANSPARENCY (TR)

*Error! Reference source not found.*

<i>TR-1 – Privacy Notice (Low)</i>	<i>PI</i>
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;</i></li> <li><i>b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and</i></li> <li><i>c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.</i></li> </ul>	
<p><b>Guidance</b></p> <p><i>Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.</i></p> <p><i>The organization's Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE). Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel.</i></p>	
<p><b>Reference(s):</b> <i>E-Gov: § 208(b); OMB: M-03-22, M-07-16, M-10-22, M-10-23; Privacy</i></p>	<p><b>Related Controls Requirement(s):</b> <i>AP-1,</i></p>

<i>Act: § 552a(e)(3), § 552a(e)(4)</i>	<i>AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2</i>
<b>ASSESSMENT PROCEDURE: TR-1.1</b>	
<p><b>Assessment Objective</b></p> <p><i>Determine if:</i></p> <p><i>(i) the organization provides effective notice to the public and to individuals regarding:</i></p> <p><i>(ii) the organization describes:</i></p> <ul style="list-style-type: none"> <li><i>- the PII the organization collects and the purpose(s) for which it collects that information;</i></li> <li><i>- how the organization uses PII internally;</i></li> <li><i>- whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;</i></li> <li><i>- whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;</i></li> <li><i>- how individuals may obtain access to PII;</i></li> <li><i>- how the PII will be protected;</i></li> </ul> <p><i>(iii) the organization revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.</i></p> <p><b>Assessment Methods And Objects</b></p> <p><i>Examine: Public notice regarding individual privacy and PII; other relevant documents or records.</i></p>	
<b>TR-2 – System of Records Notices and Privacy Act Statements (Low)</b>	
<p><b>Control</b></p> <p><i>The organization:</i></p> <ul style="list-style-type: none"> <li><i>a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);</i></li> <li><i>b. Keeps SORNs current; and</i></li> <li><i>c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.</i></li> </ul>	
<p><b>Guidance</b></p> <p><i>Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as “a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier.” SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or</i></p>	

<i>national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys).</i>	
<b>Reference(s):</b> OMB: Circular A-130; Privacy Act: § 552a(e)(3)	<b>Related Controls Requirement(s):</b> DI-2
<b>ASSESSMENT PROCEDURE: TR-2.1</b>	
<b>Assessment Objective</b> <i>Determine if:</i> <i>(i) the organization publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII;</i> <i>(ii) the organization keeps SORNs current;</i> <i>(iii) the organization includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.</i>	
<b>Assessment Methods And Objects</b> <i>Examine:</i> Organization SORN(s); Privacy Act Statements on forms that collect PII; Privacy Act Statements on separate forms for individuals; other relevant documents or records.	
<b>TR-3 – Dissemination of Privacy Program Information (Low)</b>	
<b>PI</b>	
<b>Control</b> <i>The organization:</i> <i>a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and</i> <i>b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.</i>	
<b>Guidance</b> <i>Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.</i>	
<b>Reference(s):</b> E-Gov: § 208; OMB: M-03-22, M-10-23; Privacy Act: § 552a	<b>Related Controls Requirement(s):</b> AR-6

***ASSESSMENT PROCEDURE: TR-3.1***

***Assessment Objective***

*Determine if:*

*(i) the organization ensures that the public has access to information about its privacy activities and is able to communicate with its SAOP/CPO;*

*(ii) the organization ensures that its privacy practices are publicly available through organizational websites or otherwise.*

***Assessment Methods And Objects***

***Examine:*** *Organization SORN(s) on public website; other relevant documents or records.*

## 26.0 USE LIMITATION (UL)

*Error! Reference source not found.*

<b>UL-1 – Internal Use (Low)</b>		<b>PI</b>
<b>Control</b>		
<i>The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.</i>		
<b>Guidance</b>		
<i>Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII.</i>		
<b>Reference(s):</b> Privacy Act: § 552a(b)(1)		<b>Related Controls Requirement(s):</b> AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2
<b>ASSESSMENT PROCEDURE: UL-1.1</b>		
<b>Assessment Objective</b>		
<i>Determine if the organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.</i>		
<b>Assessment Methods And Objects</b>		
<i><b>Examine:</b> Organization privacy policy; organization privacy practices; other relevant documents or records.</i>		
<b>UL-2 – Information Sharing with Third Parties (Low)</b>		<b>PI</b>
<b>Control</b>		
<i>The organization:</i>		
<i>a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes;</i>		
<i>b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the</i>		

*purposes for which the PII may be used;*

*c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and*

*d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.*

**Guidance**

*The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their Privacy Impact Assessments (PIA), System of Records Notices (SORN), website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.*

**Reference(s):** Privacy Act: § 552a(a)(7), § 552a(b), § 552a(c), § 552a(e)(3)(C), § 552a(o)

**Related Controls Requirement(s):** AP-2, AR-3, AR-4, AR-5, AR-8, DI-1, DI-2, IP-1, TR-1

**ASSESSMENT PROCEDURE: UL-2.1**

**Assessment Objective**

*Determine if:*

*(i) the organization shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes;*

*(ii) the organization where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;*

*(iii) the organization monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII;*

*(iv) the organization evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.*

***Assessment Methods And Objects***

***Examine:*** Organization privacy policy; organization privacy practices; Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements with third parties; system configuration; audit records; training records; other relevant documents or records.