AC-2 1 Access Control | Account Management

1. Define and document the types of accounts allowed for use within the system;
2. Assign account managers;
3. Establish condition for group and role membership;
4. Specify:
   a. Authorised users of the system;
   b. Group and role membership:
5. Access authorizations (i.e., privilege) and assignment of organization-defined attributes (as required) for each account;
6. Require approvals by organization-defined personnel or roles for requests to create accounts;
7. Create, enable, modify, disable, and remove accounts in accordance with organization-defined policy, procedures, and conditions;
8. Monitor the use of accounts;
9. Notify account managers and organization-defined personnel or roles when accounts are no longer required;
10. Access organization-defined time-period when users are terminated or transferred; and
11. Access organization-defined time-period when system usage or need to know changes for an individual;
12. Authorize access to the system based on:
   a. A valid access authorization;
   b. Interact system usage; and
13. Access organization-defined attributes (as required);
14. Review accounts for compliance with account management requirements (assignment of organization-defined access frequency);
15. Establish and implement a process for changing shared or group account credentials (if deployed) when individuals are removed from the group; and
16. Align account management processes with personnel termination and transfer processes.

AC-2 (1) 2 Access Control | Account Management

Support the management of system accounts using [Assignment: organization-defined automated mechanisms].

AC-2 (2) 2 Access Control | Account Management

Automated mechanisms include using alerts or error messaging to automatically notify account managers when users are terminated or transferred, using the system to monitor account usage, and using telephonic verification to report operational account usage.

AC-2 (3) 2 Access Control | Account Management

Management of temporary and emergency accounts includes the retrieval or disabling of such accounts automatically after a predefined time period, rather than at the convenience of the system administrator. Automatic retrieval or disabling of accounts provides a more consistent implementation.

AC-2 (4) 2 Access Control | Account Management

Account management audit records are defined in accordance with AU-3 and reviewed, analyzed, and reported in accordance with AU-4.

AC-2 (5) 2 Access Control | Account Management

Automatically audit account creation, modification, disabling, deletion, and renewal actions.

AC-2 (6) 2 Access Control | Account Management

Implementation of access control requires that the system accounts be protected from and prevent unauthorized access by unauthorized users. Access control access controls rely on two access control decisions facilitated by dynamic privilege management such as attribute-based access control. While user identities remain relatively constant over time, user privileges typically change more frequently than physical access or business requirements and operational needs of organizations. An example of dynamic privilege management is the incremental revocation of privileges from users, or in response to an event that impacts access. Dynamic privilege management can include new access privileges or other attributes by account, by type of account, or a combination of the two. Examples of dynamic privilege management include accounts that are no longer required, accounts that are no longer needed, and accounts that are no longer used. Dynamic privilege management provides a more consistent implementation.
AC-2 [17] 2 Access Control / Account Management / Privileged User Accounts
(3) Enforce mandatory access control policies that exist at the system level and recognize that systems can host many applications and services in support of missions and business functions; access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

AC-3 [18] 2 Access Control / Account Management / Mandatory Access Control
(1) Establish and administer mandatory access control policy over the set of covered subjects and objects to which the system has control; otherwise, the access control policy can be circumvented. This enforcement is provided by an implementation that meets the reference implementation requirements.

AC-6 [21] 2 Access Control / Access Enforcement
(1) Establish mandatory access control policy and the set of covered subjects and objects specified in the policy, and where the policy: (a) is uniformly enforced across the covered subjects and objects within the system; (b) specifies that a subject that has been granted access to information is constrained from doing any of the following: (1) passing the information to unauthorized users or objects; (2) changing its privileges to other subjects; (3) changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components; (4) changing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and (5) specifying the roles governing access control; and (c) specifies that (Assignment: organization-defined mandatory access control strategy) such that they are not limited by any defined subset or all of the above constraints.

Notes
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Revised Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-3 (4)</td>
<td>2</td>
<td>Access Control / Access Enforcement</td>
<td>X</td>
<td>Enforce Application Access (Assignment: organization-defined security-relevant information) except during secure, non-operable system states.</td>
<td>When discretionary access control policies are implemented, subjects are not constrained regarding which subjects they can take with information for which they have already been granted access to. Thus, subjects that have been granted access to information are not prevented from passing the information to other subjects or objects (i.e., subjects have the discretion to pass). Discretionary access control can operate in conjunction with mandatory access control as described in AC-3(2) and AC-3(3). A subject that is constrained in its operation by mandatory access control policies can still operate under the less rigorous constraints of discretionary access control. Therefore, under AC-3(3) imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level. AC-3(4) permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the system. Once the information is passed outside of system control, additional means may be required to ensure that the constraints remain in effect. While traditional definitions of discretionary access control require identity-based access control, this definition is not required for this particular use of discretionary access control.</td>
<td>NE-6, SC-38</td>
<td></td>
</tr>
<tr>
<td>AC-3 (5)</td>
<td>2</td>
<td>Access Control / Protection of Specific Information Systems</td>
<td>X</td>
<td>Enforce Application Access (Assignment: organization-defined security-relevant information) except during secure, non-operable system states.</td>
<td>When discretionary access control policies are implemented, subjects are not constrained regarding which subjects they can take with information for which they have already been granted access to. Thus, subjects that have been granted access to information are not prevented from passing the information to other subjects or objects (i.e., subjects have the discretion to pass). Discretionary access control can operate in conjunction with mandatory access control as described in AC-3(2) and AC-3(3). A subject that is constrained in its operation by mandatory access control policies can still operate under the less rigorous constraints of discretionary access control. Therefore, under AC-3(3) imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level. AC-3(4) permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the system. Once the information is passed outside of system control, additional means may be required to ensure that the constraints remain in effect. While traditional definitions of discretionary access control require identity-based access control, this definition is not required for this particular use of discretionary access control.</td>
<td>NE-6, SC-38</td>
<td></td>
</tr>
<tr>
<td>AC-3 (6)</td>
<td>2</td>
<td>Access Control / Access Enforcement</td>
<td>Role-based Access Control</td>
<td>Enforce a role-based access control policy non-defined subjects and objects and control access based upon (Assignment: organization-defined roles and users authorized to assume such roles). Role-based access control (RBAC) is an access control policy that enforces access to subjects and system functions based on the defined role (i.e., job) function) of the subject. Organizations can create specific roles based on job functions and the authorizations [i.e., privileges] or perform operations on the systems associated with the organization-defined rules. When users are assigned to the specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration because privileges are not assigned directly to every user (which can potentially be a large number of individuals) but are instead acquired through role assignments. RBAC can be implemented as both mandatory or discretionary forms of access control. For those organizations implementing RBAC with mandatory access controls, the requirements in AC-3(6) define the scope of the subjects and objects covered by the policy.</td>
<td>Enforce a role-based access control policy non-defined subjects and objects and control access based upon (Assignment: organization-defined roles and users authorized to assume such roles). Role-based access control (RBAC) is an access control policy that enforces access to subjects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations [i.e., privileges] or perform operations on the systems associated with the organization-defined rules. When users are assigned to the specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration because privileges are not assigned directly to every user (which can potentially be a large number of individuals) but are instead acquired through role assignments. RBAC can be implemented as both mandatory or discretionary forms of access control. For those organizations implementing RBAC with mandatory access controls, the requirements in AC-3(6) define the scope of the subjects and objects covered by the policy.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>AC-3 (7)</td>
<td>2</td>
<td>Access Control / Access Enforcement</td>
<td>Revocation of Access Authorizations</td>
<td>Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on (Assignment: organization-defined rules governing the timing of revocations of access authorizations). Revocation of access rules may differ based on the type of access model. For example, if a subject (i.e., user or process acting on behalf of a user) is removed from a group, access may not be revoked until the next time the subject attempts to make a request to the object. The revocation process is necessary to ensure that access is properly monitored and controlled.</td>
<td>Revocation of access rules may differ based on the type of access model. For example, if a subject (i.e., user or process acting on behalf of a user) is removed from a group, access may not be revoked until the next time the subject attempts to make a request to the object. The revocation process is necessary to ensure that access is properly monitored and controlled.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>AC-3 (8)</td>
<td>2</td>
<td>Access Control / Access Enforcement</td>
<td>Controlled Release</td>
<td>Release information outside of the system only if: (a) The receiving organization (organization-defined system or system component) provides (Assignment: organization-defined controls), and (Assignment: organization-defined controls) are used to validate the appropriateness of the information access for release. Systems can only protect organizational information within the confines of established system boundaries. Additional controls may be needed to ensure that such information is adequately protected once it is passed beyond the established system boundaries. In situations where the system is unable to determine the suitability of the protection provided by external entities, as a mitigating control, organizations determine procedurally whether the external systems are providing adequate controls. The means used to determine the suitability of controls provided by external systems include conducting periodic assessments (inspections) and establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need to be as strong as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals’ privacy. Controlled release of information requires systems to implement technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to a system controlled by another organization, technical means are employed to validate that the security and privacy attributes associated with the exported information do not exceed the sensitivity or privacy limits of the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only authorized individuals gain access to the printer.</td>
<td>Release information outside of the system only if: (a) The receiving organization (organization-defined system or system component) provides (Assignment: organization-defined controls), and (Assignment: organization-defined controls) are used to validate the appropriateness of the information access for release. Systems can only protect organizational information within the confines of established system boundaries. Additional controls may be needed to ensure that such information is adequately protected once it is passed beyond the established system boundaries. In situations where the system is unable to determine the suitability of the protection provided by external entities, as a mitigating control, organizations determine procedurally whether the external systems are providing adequate controls. The means used to determine the suitability of controls provided by external systems include conducting periodic assessments (inspections) and establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need to be as strong as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals’ privacy. Controlled release of information requires systems to implement technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to a system controlled by another organization, technical means are employed to validate that the security and privacy attributes associated with the exported information do not exceed the sensitivity or privacy limits of the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only authorized individuals gain access to the printer.</td>
<td>X, P-12, P-14, P-17, P-21, U-14-16, U-16-10, U-16-12, U-16-14</td>
<td></td>
</tr>
<tr>
<td>AC-3 (9)</td>
<td>2</td>
<td>Access Control / Access Enforcement</td>
<td>Audited Override of Access Control Mechanisms</td>
<td>Display an audited override of evaluated access control mechanisms wider (Assignment: organization-defined conditions) by (Assignment: organization-defined rules).</td>
<td>Display an audited override of evaluated access control mechanisms wider (Assignment: organization-defined conditions) by (Assignment: organization-defined rules).</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>AC-3 (10)</td>
<td>2</td>
<td>Access Control / Access Enforcement</td>
<td>Restrict Access to Specific Information Types</td>
<td>Restrict access to specific information types (Assignment: organization-defined information types). Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role-based access could be employed to allow access only to a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to biographical keys, authentication information, and related system information.</td>
<td>Restrict access to specific information types (Assignment: organization-defined information types). Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role-based access could be employed to allow access only to a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to biographical keys, authentication information, and related system information.</td>
<td>U-12, U-14</td>
<td></td>
</tr>
<tr>
<td>AC-3 (11)</td>
<td>2</td>
<td>Access Control / Access Enforcement</td>
<td>Asset and Exports Application Access</td>
<td>(a) Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: (Assignment: organization-defined system applications and functions), and (b) Provide an enforcement mechanism to prevent unauthorized access, and (c) Approve access changes after initial installation of the application.</td>
<td>(a) Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: (Assignment: organization-defined system applications and functions), and (b) Provide an enforcement mechanism to prevent unauthorized access, and (c) Approve access changes after initial installation of the application.</td>
<td>CM-7</td>
<td></td>
</tr>
<tr>
<td>Control ID</td>
<td>Level</td>
<td>Control Name</td>
<td>Withdrawn</td>
<td>Control Text</td>
<td>Document</td>
<td>Related Controls</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>--------------</td>
<td>----------</td>
<td>--------------</td>
<td>----------</td>
<td>----------------</td>
<td>-------</td>
</tr>
<tr>
<td>AC-3 (14)</td>
<td>2</td>
<td>Access Control</td>
<td>Access Enforcement</td>
<td></td>
<td>Attribute-based Access Control</td>
<td></td>
<td>AC-3(15) 2 Access Control</td>
</tr>
<tr>
<td>AC-3 (14)</td>
<td>2</td>
<td>Access Control</td>
<td>Access Enforcement</td>
<td>Individual Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-4 (1)</td>
<td>1</td>
<td>Access Control</td>
<td>Information Flow Enforcement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AC-4 (9) 2 Access Control | Information Flow Enforcement | Security or Privacy Policy Filters

Organizations define security or privacy policy filters for all situations where automated flow control decisions are possible. When a fully automated flow control decision is not possible, then a human reviewer may be employed to rule on it, or as a complement to, automated security or privacy policy filtering. Human reviews may also be employed as deemed necessary by organizations.

AC-4 (11) 2 Access Control | Information Flow Enforcement | Configuration of Security or Privacy Policy Filters

Document retention contains detailed information for configuring security or privacy policy filters. For example, administrators can configure security or privacy policy filters to include the list of "dirty words" that security or privacy policy mechanisms check in accordance with the definitions provided to organizations.

AC-4 (12) 2 Access Control | Information Flow Enforcement | Data Type Identification

Data type-identifiers include filenames, the map, the signature, or tokens, and multiple integral file signatures or tokens. Systems allow transfer of data only if it complies with data type format specifications. Identification and validation of data types is based on defined specifications associated with each allowed data format. The filename and number alone are not useful for data type identification. Content is validated syntactically and semantically against its specifications to ensure it is the proper data type.

AC-4 (13) 2 Access Control | Information Flow Enforcement | Decomposition into Policy-relevant Subcomponents

Decomposition of different security or privacy domains, decompose information into assignments of organization-defined policy-relevant subcomponents for dissemination to policy enforcement mechanisms.

AC-4 (14) 2 Access Control | Information Flow Enforcement | Security or Privacy Policy Filter Cavators

When transferring information between different security or privacy domains, implement assignment of organization-defined security or privacy policy filters requiring fully enumerated formats that restrict data structure and content.

AC-4 (15) 2 Access Control | Information Flow Enforcement | Detection of Unanticipated Information

When transferring information between different security or privacy domains, examine the information for the presence of assignment of organization-defined unanticipated information) and prohibit the transfer of such information in accordance with the assignment of organization-defined security or privacy policy.

AC-4 (16) 2 Access Control | Information Flow Enforcement | Information Transfers to Interconnected Systems

Uniquely identify and authenticate source and destination points by assigning (one or more) organizational, system, application, service, individual, or identification transfer.

AC-4 (17) 2 Access Control | Information Flow Enforcement | Domain Authorization

Domain authorization includes identifying and authorizing sources and destinations points by assigning (one or more): organizational, system, application, service, individual, or identification transfer.

AC-4 (18) 2 Access Control | Information Flow Enforcement | Security Attribute Security

Security attribute security includes identifying and authorizing sources and destinations points by assigning (one or more): organizational, system, application, service, individual, or identification transfer.

AC-4 (19) 2 Access Control | Information Flow Enforcement | Resolution of Metanets

When transferring information between different security or privacy domains, implement assignment of organization-defined security or privacy policy filters on metanets.

AC-4 (20) 2 Access Control | Information Flow Enforcement | Approved Solutions

Enforce assignment of organization-defined solutions to approved configurations to control the flow of assignment of organization-defined information across security or privacy domains.

Organizations define approved solutions and configurations in cross domain policies and guidance in accordance with the type of information flow across classification boundaries. The NAC National Cross Domain Strategy and Management Office provides a descriptive listing of approved cross domain solutions.
AC-4 (11) 2 Access Control / Information Flow Enforcement | Physical or logical separation of Information Flows | separate information flows logically or physically using assignment: organization-defined mechanisms and techniques to accomplish [assignment: organization-defined required separations by type of information].

AC-4 (12) 2 Access Control / Information Flow Enforcement | Access Only | Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing any information flow between the different security domains.

The system provides a capability for users to access each connected security domain without providing any mechanisms to alter transfer of data or information between the different security domains. An example of an access-only solution is a terminal that provides a user access to information with different security classifications while preventing the information separate.

AC-4 (13) 2 Access Control / Information Flow Enforcement | Identify non-releasable information | When transferring information between different security domains, modify or non-releasable information by implementing [assignment: organization-defined modification actions].

Modifying non-releasable information can help prevent a data spill or attack when information is transferred across security domains. Modification actions include masking, perturbation, alteration, removal, or redaction.

AC-4 (14) 2 Access Control / Information Flow Enforcement | Internal Normalized Format | When transferring information between different security domains, ensure data en route is internal normalized format and ensure data is able to be transferred between different information assurance systems.

Coversion into the normalized form is one of the most effective mechanisms to stop malicious attacks and larger classes of data infiltration.

AC-4 (15) 2 Access Control / Information Flow Enforcement | Data Sanitization | When transferring information between different security domains, record and audit current filtering actions and results for the information being filtered.

Content filtering is the process of inspecting information as it traverses a cross domain solution and determines if the information meets a pre-defined policy. The use of lower content filter pipelines ensures that filter processing is non-loopable and always isolated. In general, the use of parallel filtering architectures for content filtering of a single data type introduces by-pass and non-intrusion issues.

AC-4 (17) 2 Access Control / Information Flow Enforcement | Redundant/Independent Filtering Mechanisms | When transferring information between different security or privacy domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.

Content filtering is the process of inspecting information as it traverses a cross domain solution and determines if the information meets a pre-defined policy. Redundant and independent content filtering mechanisms eliminate a single point of failure filtering system. Independence is defined as implementation of content filter that use a different code base and supporting libraries (e.g., two JPEG filters using different vendors' JPEG libraries) and multiple, independent system processes.

AC-4 (20) 2 Access Control / Information Flow Enforcement | User Filter Patches | When transferring information between different security or privacy domains, implement a linear content filter engine that is enforced with discretionary and mandatory access control.

Content filtering is the process of inspecting information as it traverses a cross domain solution and determines if the information meets a pre-defined policy. Content filtering is the process of inspecting information as it traverses a cross domain solution and determines if the information meets a pre-defined policy. An example of a content filter engine is one that performs content filtering in parallel to the security domain.

AC-4 (21) 2 Access Control / Information Flow Enforcement | Filter Orchestration Engines | When transferring information between different security or privacy domains, employ content filter orchestration engines to ensure that:

(a) Content filtering mechanisms successfully complete execution without errors; and
(b) Content filtering actions occur in the correct order and comply with [assignment: organization-defined policy].

Content filtering is the process of inspecting information as it traverses a cross domain solution and determines if the information meets a pre-defined policy. Content filtering is the process of inspecting information as it traverses a cross domain solution and determines if the information meets a pre-defined policy. An example of a filter orchestration is one that performs content filtering in parallel to the security domain.

AC-4 (22) 2 Access Control / Information Flow Enforcement | Packet Filter Pipelines | When transferring information between different security or privacy domains, implement content filtering mechanisms using multiple processes, roles, and accounts as necessary, to achieve least privilege.

The use of multiple processes to implement content filtering mechanisms reduces the chances of a process failure affecting the entire security domain. Analyzing multiple, independent system processes.

AC-4 (23) 2 Access Control / Information Flow Enforcement | Process Requirements for Information Transfer | When transferring information between different security or privacy domains, the processes that transfer information between filter pipelines:

(a) Does not filter message content;
(b) Relates filtering mechanisms; and
(c) Ensures the content associated with the filtering mechanisms has successfully completed filtering; and
(d) Transfers the content to the destination filter pipeline.

The processes transferring information between filter pipelines have minimum complexity and functionality to provide assurance that the processes operate correctly.

AC-5 1 Access Control | Separation of Duties | a. Identify and document [assignment: organization-defined duties of individuals requiring separation]; and
b. Define system access authorizations to support separation of duties.

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malvolent activity without collusion. Separation of duties includes isolating mission or business functions and support functions among different individuals or roles; conducting system support functions with different individuals; and ensuring security personnel managing access control functions do not also administer audit functions. Because separation of duty violations can open systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. This control is enforced through the account management activities in AC-2 and access control mechanisms in AC-3.

AC-6 1 Access Control | Least Privilege | Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes required to operate at privilege levels no higher than necessary to accomplish organizational mission or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary, to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

AC-6 (1) 2 Access Control | Least Privilege | Administrator Access to Security Functions | Accountability authorizes for [assignment: organization-defined individuals or roles to:
(a) [assignment: organization-defined security functions (e.g., change system state, change software, and firewall)]; and
(b) [assignment: organization-defined security-related information].

Security functions include establishing system accounts; configuring access authorizations (i.e., permissions, privileges), configuring settings for users to be audited, and establishing intrusion detection parameters. Security-related information includes filtering rules for inputs or forwards, configuration parameters for security services, cryptographic key management information, and access control lists. Legitimately authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

AC-6 (2) 2 Access Control | Least Privilege | Non-privileged Access for Nonsecurity Functions | Require that users of system accounts (or roles) with access to [assignment: organization-defined security functions or security-related information], use non-privileged accounts or roles, when accessing nonsecurity functions.

Requiring use of non-privileged accounts when accessing nonsecurity functions limits malvolent behavior operating from within privileged accounts or roles. The existence of non-privileged situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Text</th>
<th>Withdrawn</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-4 (5)</td>
<td>2</td>
<td>Access Control</td>
<td>Privileged Accounts</td>
<td>Restrict privileged accounts in the system to [assignment: organization-defined personnel or role].</td>
<td>AC-2, MA-3, MA-4</td>
</tr>
<tr>
<td>AC-4 (5)</td>
<td>2</td>
<td>Access Control</td>
<td>Non-organizational Users</td>
<td>Offer non-privileged access to the system by non-organizational users.</td>
<td>AC-5, IA-8, AU-3, AU-12</td>
</tr>
<tr>
<td>AC-4 (5)</td>
<td>2</td>
<td>Access Control</td>
<td>Privilege Levels for Code Execution</td>
<td>Prevent the following software from executing at higher privilege levels than users executing the software: [assignment: organization-defined software].</td>
<td>AC-3, AC-5, AU-2, AU-5</td>
</tr>
<tr>
<td>AC-4 (6)</td>
<td>2</td>
<td>Access Control</td>
<td>Privileged Functions</td>
<td>Audit the execution of privileged functions.</td>
<td>AC-3, AC-5, AU-2, AU-5, SC-16</td>
</tr>
<tr>
<td>AC-4 (6)</td>
<td>2</td>
<td>Access Control</td>
<td>Prohibit Non-privileged Users from Executing Privileged Functions</td>
<td>Prevent non-privileged users from executing privileged functions.</td>
<td>AC-7</td>
</tr>
<tr>
<td>AC-4 (10)</td>
<td>2</td>
<td>Access Control</td>
<td>Unsuccessful Login Attempts</td>
<td>a. Enforce a limit [assignment: organization-defined number] of unsuccessful login attempts by a user during a [assignment: organization-defined time period]; and b. Automatically lockout (livelockout) lock the account or node for an [assignment: organization-defined time period]; lock the account or node until released by an administrator; delay until login attempts are resolved; [assignment: organization-defined delay algorithm]; notify system administrator; take other [assignment: organization-defined action] when the maximum number of unsuccessful attempts is exceeded.</td>
<td>AC-3, AC-5, AU-2, AU-5, SC-16, SC-18</td>
</tr>
<tr>
<td>AC-6 (2)</td>
<td>2</td>
<td>Access Control</td>
<td>Access Control</td>
<td>Prevent non-privileged access to any network access in the system to network access to [assignment: organization-defined privileged commodity] only for [assignment: organization-defined personnel or role] for the network.</td>
<td>AC-3, AC-5, AU-2, AU-5, SC-16, SC-18</td>
</tr>
<tr>
<td>AC-6 (2)</td>
<td>2</td>
<td>Access Control</td>
<td>Access Control</td>
<td>Implement separate physical domains for fine-grained allocation of user privileges. Providing separate physical domains for fine-grained allocation of user privileges includes using segmentation techniques to permit additional user privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying physical machine, implementing separate physical domains, and employing hardware or software domain separation mechanisms.</td>
<td>AC-3, AC-5, AU-2, AU-5, SC-16, SC-18</td>
</tr>
</tbody>
</table>
AC-7 (4)  |  2 | Access Control | Unsuccessful Logon Attempts / Use of Alternate Factor |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Display (Assignment: organization-defined authentication factors) that are different from the primary authentication factors after the number of organization defined consecutive invalid login attempts have been reached; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Inform the users of (Assignment: organization-defined number) consecutive invalid login attempts through use of the alternative factors by a user during a (Assignment: organization-defined time period).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The use of alternate authentication factors supports the objective of availability and allows a user that has intermittently been locked out to use additional authentication factors to bypass theinct.

AC-8  |  1 | Access Control | System Use Notification |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Display ( Assignment: organization-defined system use notification message or banner) to users before granting access to the system that provides privacy and security notice consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Users are accessing a U.S. Government 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; and
- Use of the system indicates consent to monitoring and recording. |

If the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log off or to further access the system; and
- For publicly accessible systems:
  1. Display system use information (Assignment: organization-defined conditions), before granting further access to the publicly accessible system;
  2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
  3. Include a description of the authorized uses of the system. |

System-use notifications can be implemented using messages or warning banners displayed before individuals log into systems. System-use notifications are used only for access via logins interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network login. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

AC-9  |  1 | Access Control | Previous Login Notification |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify the user, upon successful logon to the system, of the date and time of the last logon.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Previous login notification is applicable to system access via human user interfaces and access to systems that occurs in other types of architectures. Information about the last successful login allows the user to recognize if the date and time provided is not consistent with the user's last access.

AC-10  |  2 | Access Control | Concurrent Session Control |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Prevent further access to the system by selecting [one or more] initiating a device lock after (Assignment: organization-defined time period) of inactivity, requiring the user to initiate a device lock before leaving the system unattended; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Prevent the device lock until the user reestablishes access using established identification and authentication procedures.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Device locks are temporary actions taken to prevent logical access to organizational systems when users step away and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User initiated device locking is behavior or policy based and as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging off of systems, for example, Internet Protocol (IP) addresses from which network logons occurred, notifications of local logons, or device identifiers.

AC-11  |  2 | Access Control | Device Lock |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Prevent further access to the system by selecting [one or more] initiating a device lock after (Assignment: organization-defined time period) of inactivity, requiring the user to initiate a device lock before leaving the system unattended; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Prevent the device lock until the user reestablishes access using established identification and authentication procedures.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Device locks are temporary actions taken to prevent logical access to organizational systems when users step away and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User initiated device locking is behavior or policy based and as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging off of systems, for example, Internet Protocol (IP) addresses from which network logons occurred, notifications of local logons, or device identifiers.

AC-12  |  1 | Access Control | Session Termination |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically terminate a user session after (Assignment: organization-defined conditions or trigger events requiring session disconnection).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnections). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user’s logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on systems use.

AC-13  |  2 | Access Control | Session Termination / User-related Logouts |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to (Assignment: organization-defined information resources).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information resources to which users gain access via authentication include local authorizations, directories, and password-protected websites or web-based services.

AC-14  |  2 | Access Control | Session Termination / User-related Logouts |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Display an explicit logout message to users indicating the termination of authenticated communications sessions.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logout messages for web access can be displayed after authenticated sessions have been terminated. However, for certain types of sessions, including file transfers protocols (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.

AC-15  |  1 | Access Control | Supervisory and Review — Access Control |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Withdrawn: Incorporated into AC-2, AC-6.
AC-14 1 Access Control | Permitted Actions Without Identification or Authentication

- Define the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] with information in storage, in process, and/or in transmission.
- Ensure that the attribute associations are made and retained with the information.
- Establish the permitted [Assignment: organization-defined security and privacy attribute values] for [Assignment: organization-defined types of security and privacy attributes] for [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).
- Determine the permitted [Assignment: organization-defined values or ranges] for each of the established attributes.
- Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to authorized individuals.
- Audit changes to attributes; and
- Determine the permitted [Assignment: organization-defined values or ranges] for each of the established attributes.

Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication is not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publically accessible federal systems; when individual use mobile phones to receive calls; or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may under certain circumstances, 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 login functionality and is protected from accidental or unauthorized 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 an organizational system without identification and authentication and therefore, the value for the assignment can be zero.

AC-15 Access Control | Access Control Management

- Define the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] with information in storage, in process, and/or in transmission.
- Ensure that the attribute associations are made and retained with the information.
- Establish the permitted [Assignment: organization-defined security and privacy attribute values] for [Assignment: organization-defined types of security and privacy attributes] for [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).
- Determine the permitted [Assignment: organization-defined values or ranges] for each of the established attributes.
- Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to authorized individuals.
- Audit changes to attributes; and
- Determine the permitted [Assignment: organization-defined values or ranges] for each of the established attributes.

Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication is not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publically accessible federal systems; when individual use mobile phones to receive calls; or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may under certain circumstances, 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 login functionality and is protected from accidental or unauthorized 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 an organizational system without identification and authentication and therefore, the value for the assignment can be zero.

OCCM Control Set for NIST SP 800-53 rev. 5 Final Public Draft

Page 9 of 108
Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

Remote access is access to organizational systems (or processes acting on behalf of users) by users other than authorized users (e.g., systems from external networks), including systems acting on behalf of users who are members of the organization. Typically, remote access allows users to access the organization’s computing resources (such as workstations, servers, databases, and printers) that they would not have access to if they were physically present in the same location as the computing resources. Remote access to organizational systems can be used to provide employees with access to their workstations and computing resources, even when they are remote from the office (e.g., telecommuters). Remote access capabilities often include authentication of users and devices with encryption to reduce susceptibility to threats by adversaries exploiting wireless technologies. Remote access can include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote communications. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively trust such communications as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, standards, and guidelines. Strong VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote communications. Use of encrypted VPNs can also affect the capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the specific format(s) for such authorization. While organizations may use information exchange and system connection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote access is addressed via AC-1.

Remote access to organizational systems (or processes acting on behalf of users) by users other than authorized users (e.g., systems from external networks), including systems acting on behalf of users who are members of the organization. Typically, remote access allows users to access the organization’s computing resources (such as workstations, servers, databases, and printers) that they would not have access to if they were physically present in the same location as the computing resources. Remote access to organizational systems can be used to provide employees with access to their workstations and computing resources, even when they are remote from the office (e.g., telecommuters). Remote access capabilities often include authentication of users and devices with encryption to reduce susceptibility to threats by adversaries exploiting wireless technologies. Remote access can include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote communications. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively trust such communications as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, standards, and guidelines. Strong VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote communications. Use of encrypted VPNs can also affect the capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the specific format(s) for such authorization. While organizations may use information exchange and system connection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote access is addressed via AC-1.

Remote access to organizational systems (or processes acting on behalf of users) by users other than authorized users (e.g., systems from external networks), including systems acting on behalf of users who are members of the organization. Typically, remote access allows users to access the organization’s computing resources (such as workstations, servers, databases, and printers) that they would not have access to if they were physically present in the same location as the computing resources. Remote access to organizational systems can be used to provide employees with access to their workstations and computing resources, even when they are remote from the office (e.g., telecommuters). Remote access capabilities often include authentication of users and devices with encryption to reduce susceptibility to threats by adversaries exploiting wireless technologies. Remote access can include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote communications. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively trust such communications as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, standards, and guidelines. Strong VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote communications. Use of encrypted VPNs can also affect the capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the specific format(s) for such authorization. While organizations may use information exchange and system connection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote access is addressed via AC-1.
AC-19 1 Access Control | Access Control for Mobile Devices

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

A mobile device is a computing device that has a small form factor such that it can easily be carried. A mobile device may be a single individual's device designed to operate without a physical connection; possesses local, removable or removable data storage; and includes a self-contained power source. Mobile device functionality 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 and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or nearly a subset of a notebook/desktop system, depending upon the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect mobile devices when outside of controlled areas. Controlled areas are specific for which organizations provide physical or procedural controls to meet the requirements established for processing information and systems. Mobile devices can easily be subject to theft, loss, or tampering, thereby potentially compromising the confidentiality and integrity of information handled by the mobile device (including resident software) integrity checks, and disabling unnecessary hardware.

Configuration restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective profiles, secure boot processes for hardware and operating system, and identity/change authentication. Steps are necessary to protect mobile devices from being connected to unauthorized systems and to ensure that their configuration requirements are met. Unless otherwise specified, configuration requirements apply to both classified and unclassified mobile devices. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or nearly a subset of a notebook/desktop system, depending upon the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect mobile devices when outside of controlled areas. Controlled areas are specific for which organizations provide physical or procedural controls to meet the requirements established for processing information and systems. Mobile devices can easily be subject to theft, loss, or tampering, thereby potentially compromising the confidentiality and integrity of information handled by the mobile device (including resident software) integrity checks, and disabling unnecessary hardware.

Configuration restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective profiles, secure boot processes for hardware and operating system, and identity/change authentication. Steps are necessary to protect mobile devices from being connected to unauthorized systems and to ensure that their configuration requirements are met. Unless otherwise specified, configuration requirements apply to both classified and unclassified mobile devices. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or nearly a subset of a notebook/desktop system, depending upon the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect mobile devices when outside of controlled areas. Controlled areas are specific for which organizations provide physical or procedural controls to meet the requirements established for processing information and systems. Mobile devices can easily be subject to theft, loss, or tampering, thereby potentially compromising the confidentiality and integrity of information handled by the mobile device (including resident software) integrity checks, and disabling unnecessary hardware.

Configuration restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective profiles, secure boot processes for hardware and operating system, and identity/change authentication. Steps are necessary to protect mobile devices from being connected to unauthorized systems and to ensure that their configuration requirements are met. Unless otherwise specified, configuration requirements apply to both classified and unclassified mobile devices. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or nearly a subset of a notebook/desktop system, depending upon the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect mobile devices when outside of controlled areas. Controlled areas are specific for which organizations provide physical or procedural controls to meet the requirements established for processing information and systems. Mobile devices can easily be subject to theft, loss, or tampering, thereby potentially compromising the confidentiality and integrity of information handled by the mobile device (including resident software) integrity checks, and disabling unnecessary hardware.

Configuration restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective profiles, secure boot processes for hardware and operating system, and identity/change authentication. Steps are necessary to protect mobile devices from being connected to unauthorized systems and to ensure that their configuration requirements are met. Unless otherwise specified, configuration requirements apply to both classified and unclassified mobile devices. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or nearly a subset of a notebook/desktop system, depending upon the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect mobile devices when outside of controlled areas. Controlled areas are specific for which organizations provide physical or procedural controls to meet the requirements established for processing information and systems. Mobile devices can easily be subject to theft, loss, or tampering, thereby potentially compromising the confidentiality and integrity of information handled by the mobile device (including resident software) integrity checks, and disabling unnecessary hardware.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-20</td>
<td>1</td>
<td>Accurate Control</td>
<td>Use of External Systems</td>
</tr>
<tr>
<td>AC-20 (1)</td>
<td></td>
<td>Access Control / Use of External Systems</td>
<td>Permit authorized individuals to use an external system to access the system or to process, store, or transmit non-organizationally owned systems or system components to process, store, or transmit organization-controlled information using [assignment: organization-defined requirements].</td>
</tr>
<tr>
<td>AC-20 (2)</td>
<td></td>
<td>Access Control / Use of External Systems - Prohibited Use</td>
<td>Prohibit the use of non-organizationally owned systems or system components owned by other organizations and personally owned devices. There are potential risks to using non-organizationally owned systems or system components. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, the use of such systems or system components may be allowed but restricted in some way. Restrictions include requiring the implementation of improved controls prior to authorizing connection of non-organizationally owned systems and components; limiting access to types of information; services, or applications; using authentication techniques to limit processing and storage activities to servers or system components provided by the organization; and adjusting the terms and conditions of use. Organizations consult with the Office of the General Counsel regarding legal issues associated with using personally owned devices, including requirements for conducting incident analysis or investigations after an incident.</td>
</tr>
<tr>
<td>AC-21</td>
<td></td>
<td>Access Control / Information Sharing</td>
<td>Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include: contracted work, classified information, proprietary information and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing patterns may be defined at the individual, group, or organizational level. Information may be defined by context, type, security category, or special access program or compartments. Access restrictions may include non-disclosure agreements (NDAs).</td>
</tr>
<tr>
<td>AC-22</td>
<td></td>
<td>Access Control / Publicly Accessible Content</td>
<td>In accordance with applicable laws, executive orders, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the Federal Records Act and proprietary information. This control addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizationally systems, such as, non-organizationally public websites, forums, and social media is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, this control addresses the management of the individuals who make such information publicly accessible.</td>
</tr>
</tbody>
</table>
AC-23  1  Access Control | Data Mining Protection

Implement a reference monitor for [Assignment: organization-defined access control policies] that is
[Selection: Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access
control decisions] are applied to each access request prior to access enforcement.

Data mining is an analytical process that attempts to find correlations or patterns in large
data sets for the purpose of data or knowledge discovery. Data storage objects include
database records and database fields. Sensitive information can be extracted from data
mining operations. When information is personally identifiable information, it may lead to
extrapolation revelations about individuals and give rise to privacy risks. Prior to
performing data mining activities, organizations determine whether such activities are
authorized. Organizations may be subject to applicable laws, executive orders, directives,
regulations, or policies that address data mining requirements. Organizational personnel
consult with the senior agency official for privacy and legal counsel regarding such
requirements.

Data-mining prevention and detection techniques include limiting the number and the
frequency of database queries to increase the work factor needed to determine the
contents of such databases, limiting types of responses provided to database queries;
applying differential privacy techniques or homomorphic encryption; and nonfiling
personnel when analytical database queries or accesses occur. Data-mining protection
focuses on protecting information from data mining while such information resides in
organizational data stores. In contrast, AC-13 focuses on monitoring for organizational
information that may have been mishandled or otherwise obtained from data stores and is
available as open source information residing on external sites, for example, through social
networking or social media websites.

[EO 13587] requires the establishment of an insider threat program for detecting,
deterring, and mitigating insider threats, including the safeguarding of sensitive information
from exploitation, compromise, or other unauthorized disclosure. This control requires
organizations to identify appropriate techniques to prevent and detect unauthorized
or unauthorized data mining; which can be used by an insider to collect organizational
information for the purpose of exfiltration.

AC-24  1  Access Control | Access Control Decisions

Select: Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access
control decisions] are applied to each access request prior to access enforcement.

Access control decisions [also known as authorization decisions] occur when authorization
information is applied to specific accesses. In contrast, access enforcement occurs when
systems enforce access control decisions. While it is very common to have access control
decisions and access enforcement implemented by the same entity, it is not required, and it
is never an optimal implementation choice. For some architectures and distributed
systems, different entities may perform access control decisions and access enforcement.

AC-24 (1) 2 Access Control | Access Control Decisions | Trusted Access Information

Transmit [Assignment: organization-defined access authorization information] using [Assignment: organization-
defined controls] to [Assignment: organization-defined systems] that enforce access control decisions.

Authorization processes and access control decisions may occur in separate parts of systems
or in separate systems. In such instances, authorization information is transported securely
(e.g., using cryptographic mechanisms) so timely access control decisions can be enforced
at the appropriate locations.

Restating controls does not constitute an organizational policy or procedure.

AC-24 (2) 2 Access Control | Access Control Decisions | No User or Process Identity

[Assignment: organization-defined security or privacy attributes] that do not include the identity of the user or
process acting on behalf of the user.

In certain situations, it is important that access control decisions can be made without
regard to the identity of the user issuing the request. There are generally instances where preserving individual privacy
is of paramount importance. In other situations, user identification information is simply not needed for access control decisions
and, especially in the case of distributed systems, transporting such information with the
needed degree of assurance may be very expensive or difficult to accomplish. MAC, MAC-
based and label-based controls, for example, might not include user identity as an
attribute.

AC-25  1  Access Control | Reference Monitor

Implement a reference monitor for [Assignment: organization-defined access control policies] that is
temporary; always invoked; and small enough to be subject to analysis and testing, the completeness of which
may be assured.

This control addresses policy and procedures for the controls in the AT family implemented
within systems and organizations. The risk management strategy is an important factor in
establishing such policies and procedures. Policies and procedures help provide security and
privacy assurance. Therefore, it is important that security and privacy programs collaborate
on their development. Security and privacy program policies and procedures at the
organization level are preferable, in general, and may obviate the need for system-specific
policies and procedures. The policies can be included as part of the general security
and privacy policy or can be represented by multiple policies reflecting the complex nature
of organizations. Procedures can be established for security and privacy programs and for
systems, if needed. Procedures describe how the policies or controls are implemented and
can be directed at the individual or role that is the object of the procedure. Procedures
can be documented in system security and privacy plans or in one or more separate documents.
Restating controls does not constitute an organizational policy or procedure.

AC-25  Notes

Notes
At-12 [2] 2 Awareness and Training | Awareness Training

Practical Exercises

Provide practical exercises in awareness training that simulate events and incidents.

Practical exercises include no-vector social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments, or invoking, via spear-phishing attacks, malicious web links.

At-12 [2] 2 Awareness and Training | Awareness Training

Breach

Provide awareness training on recognizing and reporting potential indicators of insider threat.

Potential indicators and possible precautions of insider threat can include behaviors such as: unusual, long-term job absences; attempts to gain access to information not required for job performance; unusual access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Awareness training includes how to communicate concerns of employees and management regarding potential indications of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider training insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

At-12 [2] 2 Awareness and Training | Awareness Training

Social Engineering and Mining

Provide awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.

Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, and other possible tricks, including social authenticity, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Awareness training includes information on how to communicate concerns of employees and management regarding potential indications of social engineering and social mining through organizational channels based on established policies and procedures.

At-12 [4] 2 Awareness and Training | Awareness Training

Suspicious Communications and Anomalous System Behavior

Provide awareness training on recognizing suspicious communications and anomalous behavior in organizational systems using (assignment: organization-defined indicators of malicious code).

A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indicators of potentially malicious email (e.g., receiving an unexpected email, receiving an email containing strange or garbled language, or receiving an email from a seemingly benign sender that appears to be from a known sponsor or contractor). Personnel are also trained to look for suspicious email or web communications. For this purpose to work effectively, personnel are trained and made aware of what constitutes suspicious communication. Training personnel on how to recognize anomalies demonstrated in systems can provide organizations with early warning for the presence of malicious code. Description of anomalous behavior by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.

At-2 [2] 2 Awareness and Training | Awareness Training

Insider Threat

Provide awareness training on identifying and responding to a breach, including the organization’s process for reporting a breach.

A breach is a type of incident that involves personally identifiable information. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an unauthorized user accesses or potentially accesses such information for other than authorized purposes. The awareness training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, and, or, electronic. Awareness training includes training exercise that simulate a breach.

At-2 [2] 2 Awareness and Training | Awareness Training

Advanced Persistent Threat

Provide awareness training on advanced persistent threat.

An effective way to detect advanced persistent threats (APT) and to preclude success attacks is to provide specific awareness training for individuals. Threat awareness training includes educating individuals on the serious way APTs can infiltrate into the organization (e.g., through websites, emails, advertisement pop-ups, articles, and social engineering). Effective training includes techniques for recognizing suspicious emails, use of removable systems in non-secure settings, and the potential targeting of individuals at home.

At-2 [2] 2 Awareness and Training | Awareness Training

Cyber Threat Environment

(a) Provide awareness training on the cyber threat environment; and (b) Defend current cyber threat information in system operations.

Since threats continue to change over time, the threat awareness training by the organization is dynamic. Moreover, threat awareness training is not performed in isolation from the system operations that support organizational missions and business functions.

At-2 [3] 2 Awareness and Training | Awareness Training

Training Feedback

Provide feedback on organizational training to the following personnel (assignment: organization-defined frequency) (assignment: organization-defined personnel).

Training feedback includes awareness training results and role-based training results. Training results, especially failures of personnel in critical roles, can be indicators of a potentially serious problem. Therefore, it is important that senior managers are made aware of such situations so that they can take appropriate response actions. Training feedback supports the assessment and update of organization training described in AT-2b.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT-1</td>
<td>1</td>
<td>Awareness and Training</td>
<td></td>
<td>Provide role-based security and privacy training to personnel with the following roles and responsibilities: (Assignment: organization-defined roles and responsibilities): 1. Before authorizing access to the system, information, or performing assigned duties, and (Assignment: organization-defined frequency) thereafter; and 2. When required by system change; and b. Update role-based training (Assignment: organization-defined frequency).</td>
<td>AT-3 (4) 2 Awareness and Training</td>
<td>Disclaimer: Incorporated into PM-15 (2015)</td>
</tr>
<tr>
<td>AT-2</td>
<td>2</td>
<td>Awareness and Training</td>
<td></td>
<td>Provide (Assignment: organization-defined personnel or roles) with initial and (Assignment: organization-defined frequency) training in the employment and operation of environmental controls.</td>
<td>AT-2 (4) 2 Awareness and Training</td>
<td>Disclaimer: Incorporated into AT-2 (2016)</td>
</tr>
<tr>
<td>AT-3</td>
<td>2</td>
<td>Awareness and Training</td>
<td></td>
<td>Provide (Assignment: organization-defined personnel or roles) with initial and (Assignment: organization-defined frequency) training in the employment and operation of physical security controls.</td>
<td>Physical security controls include physical access control devices, physical intrusion and detection systems, opening and closing physical access to locations, and monitoring or surveillance equipment.</td>
<td></td>
</tr>
<tr>
<td>AT-3</td>
<td>2</td>
<td>Awareness and Training</td>
<td></td>
<td>Provide role-based training (Assignment: organization-defined personnel or roles) with initial and (Assignment: organization-defined frequency) training in the employment and operation of physical security controls.</td>
<td>Role-based training also applies to contractors providing services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training including role-based training.</td>
<td></td>
</tr>
<tr>
<td>AT-4</td>
<td>2</td>
<td>Awareness and Training</td>
<td></td>
<td>Provide practical exercises in security and privacy training that reinforce training objectives.</td>
<td>Practical exercises for security training include role-playing scenarios or role-playing exercises that address privacy and security training for security professionals and for personnel who are responsible for the security and privacy aspects of systems. Physical security training includes training for software developers that addresses training, monitoring or surveillance equipment.</td>
<td></td>
</tr>
<tr>
<td>AT-5</td>
<td>2</td>
<td>Awareness and Training</td>
<td></td>
<td>private training concerning the identification of personally identifiable information (Assignment: organization-defined personnel or roles): 1. Before authorizing access to the system, information, or performing assigned duties, and (Assignment: organization-defined frequency) thereafter; and 2. When required by system change; and b. Update role-based training (Assignment: organization-defined frequency).</td>
<td>Role-based training addresses the responsibility of individuals when accessing personally identifiable information; the organization's established rules of behavior when accessing personally identifiable information; the consequences for violating the rules of behavior; and how to respond to a breach. Role-based training helps ensure personnel comply with applicable privacy requirements and is necessary to manage privacy risk.</td>
<td></td>
</tr>
<tr>
<td>AT-6</td>
<td>2</td>
<td>Awareness and Training</td>
<td></td>
<td>Document and maintain information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and a. Document individual training records for (Assignment: organization-defined personnel or roles):</td>
<td>Documentation for specialized training may be maintained by individual repositories or the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies.</td>
<td></td>
</tr>
<tr>
<td>AT-6-1</td>
<td>1</td>
<td>Audit and Accountability</td>
<td></td>
<td>a. Develop, document, and disseminate to (Assignment: organization-defined personnel or roles): 1. Selection (one or more) organization-wide; los and business process level; system (Assignment: organization-defined personnel or roles): 2. Addressing purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 3. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; and b. Designate an (Assignment: organization-defined official) to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and 2. Review and update the current audit and accountability policy and procedures; and 3. Procedures (Assignment: organization-defined frequency).</td>
<td>This control addresses policy and procedures for the controls in the AU family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate in their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Operating controls do not constitute an organizational policy or procedure.</td>
<td></td>
</tr>
</tbody>
</table>
Audit and Accountability | Event Logging

a. Identify the types of events that the system is capable of logging in support of the audit function: (Assignment: organization-defined event types that the system is capable of logging).
b. Coordinate the event logging function with other organizational entities requiring audit-related information (goals and inform the selection criteria for events to be logged).
c. Specify the following event types for logging within the system: (Assignment: organization-defined event types (subsets of the event types defined in AU-2) along with the frequency of occurrence requiring logging for each identified event type).
d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support the fact investigations of incidents; and

Review and update the event types selected for logging (Assignment: organization-defined frequency).

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.

Audit logging process failures include, for example, software and hardware errors; reaching the maximum log file size; reaching the maximum log file size, or a file system storage limit; or an inability to log additional data due to a change in system configuration. Audit logging process failures may cause the loss of audit records. Audit logging failures are also referred to as process failures, process errors, or process exceptions.
Audit and Accountability | Response to Audit Logging Failure Events | Storage Capacity Warning

Provide a warning to [assignment: organization-defined personnel, role, and/or location] when the following audit logging failure events occur: [assignment: organization-defined personnel, role, and/or location].

Alerts provide organizations with urgent messages. Real-time alerts assist messages in information technology speed (i.e., the time from event detection to alert action in seconds or less).

Audit and Accountability | Response to Audit Logging Failure Events | Storage Capacity Warning

Provide an alert when [assignment: organization-defined personnel, role, and/or location] when the audit logging failure events occur: [assignment: organization-defined personnel, role, and/or location].

Alerts may have multiple audit logging failures distributed across multiple system components, with each failure having different storage volume capacities.

Audit and Accountability | Response to Audit Logging Failure Events | Configurable Traffic Volume Thresholds

Define configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [assignment: reject, delay] network traffic above those thresholds.

Organizations have the capability to reject or delay the processing of network communications traffic. When audit logging information about such traffic is determined to exceed the storage capacity of the system audit logging function, the rejection or delay is triggered by the established organizational traffic volume thresholds that can be adjusted based on changes to audit log storage capacity.

Audit and Accountability | Response to Audit Logging Failure Events | Shutdown on Failure

Invoke a [selection: full system shutdown, partial system shutdown, degraded operational mode with limited mission or business functionality available] in the event of [assignment: organization-defined audit logging failure], unless an alternate audit logging capability exists.

The system audit logging capability may be a short-term protection solution deployed until the failure in the primary audit logging capability is corrected. Organizations may determine that the alternate audit logging capability need only provide a subset of the primary audit logging functionality that is impacted by the failure.

Audit Record Review, Analysis, and Reporting

a. Review and analyze system audit records [assignment: organization-defined frequency] for indications of [assignment: organization-defined inappropriate or unusual activity].

Audit record review, analysis, and reporting covers information security and privacy-related failures. Audits generally require an audit success frequency and type. Audits can be formal, informal, or both.

b. Specify the permitted actions for each [selection: system process; role; user] associated with the facility when the logical access occurred, may be useful in investigations.

Organizations specify permitted actions for system processes, roles, and users associated with the facility when the logical access occurred, which may be useful in investigations.

c. Report findings to [assignment: organization-defined personnel or roles]; and

d. Review and analyze system audit records [assignment: organization-defined frequency] for indications of [assignment: organization-defined inappropriate or unusual activity].

Organizations have the capability to reject or delay the processing of network communications traffic. When audit logging information about such traffic is determined to exceed the storage capacity of the system audit logging function, the rejection or delay is triggered by the established organizational traffic volume thresholds that can be adjusted based on changes to audit log storage capacity.

Audit and Accountability | Response to Audit Logging Failure Events | Alternate Audit Logging Capability

Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that impacts [assignment: organization-defined alternate audit logging functionality].

Audit and Accountability | Response to Audit Logging Failure Events | Alternate Audit Logging Capability

Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that impacts [assignment: organization-defined alternate audit logging functionality].

Audit and Accountability | Response to Audit Logging Failure Events | Alternate Audit Logging Capability

Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that impacts [assignment: organization-defined alternate audit logging functionality].

Audit and Accountability | Response to Audit Logging Failure Events | Alternate Audit Logging Capability

Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that impacts [assignment: organization-defined alternate audit logging functionality].
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU-8 (1)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Audit Record Review, Analysis, and Reporting</td>
<td>[Assignment: organization-defined fields within audit records]. Event of interest can be identified by the content of audit records including system resources accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event successes or failures. Organizations may define event severity criteria to any degree of granularity required, for example, locations selectable by a general networking location or by specific system component.</td>
<td></td>
<td></td>
<td>Withdrawn: Incorporated into AU-4(1)</td>
</tr>
<tr>
<td>AU-7 (2)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Audit Record Review and Report Generation</td>
<td>Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].</td>
<td>Audit record reduction is a process that manipulates captured audit log information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities conducting audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timing data in the record is insufficient.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-7 (1)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Audit Record Review and Report Generation</td>
<td>Provide and implement the capability to process, sort, and search audit records, events of interest based on the following content: [Assignment: organization-defined fields within audit records].</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-8 (5)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Time Stamps</td>
<td>Use internal clock systems to generate time stamps for audit records and record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.</td>
<td>Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks. For example, clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support these capabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-8 (2)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Time Stamps</td>
<td>Synchronize with Authoritative Time Source</td>
<td>Synchronize of internal system clocks with an authoritative source provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-8 (3)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Time Stamps</td>
<td>Secondary Authoritative Time Source</td>
<td>If it may be necessary to employ geolocation information to determine that the authoritative time source is in a different geographic region.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-9 (1)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Protection of Audit Information</td>
<td>Provide audit information and audit logging tools from unauthorized access, modification, and deletion.</td>
<td>Audit information includes all information, for example, audit records, audit log settings, audit reports, and personally identifiable information. It is critical to conduct audit system activity. Audit logging tools are those programs and devices used to collect security audit logging activities. Protection of audit information focuses on technical protection and environmental protection controls.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-8 (1)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Protection of Audit Information</td>
<td>Hardware Write-once Media</td>
<td>Write audit trail to hardware-enforced, write-once media.</td>
<td>Writing audit trails to hardware-enforced, write-once media applies to the initial generation of audit trails (i.e., the collection of audit records that represent the information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. Writing audit trails to hardware-enforced, write-once media does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once media [397] media includes Compact Disk-Recordable (CD-R) and Digital Versatile Disk-Recordable (DVD-R). In contrast, the use of writeable/rewriteable media such as on tape cartridges or Universal Serial Bus (USB) drives results in write-protected, but not write-once, media.</td>
<td></td>
</tr>
<tr>
<td>AU-9 (2)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Protection of Audit Information</td>
<td>Store on Separate Physical Systems or Components</td>
<td>Spore audit records. [Assignment: organization-defined frequency]. It is a reporting that is part of a physically different system or system component than the system or component being audited.</td>
<td>Storing audit records on a separate system or system component helps to ensure that a component of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organizational audit activity. Storing audit records on separate systems or components applies to initial generation as well as backup- or long-term storage of audit records.</td>
<td></td>
</tr>
<tr>
<td>AU-8 (3)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Protection of Audit Information</td>
<td>Cryptographic Protection</td>
<td>Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.</td>
<td>Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of signed hash functions among analysts, identifies the distribution of signed hash functions among analysts, and enables the distribution of signed hash functions among analysts to be verified through the distribution of signed hash functions among analysts. The public key verifies the audit information while maintaining the confidentiality of the secret key used to generate the hash.</td>
<td></td>
</tr>
<tr>
<td>AU-9 (2)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Access by Slot Activated Privileged Users</td>
<td>Authorize access to management of audit logging functionally to only [Assignment: organization-defined fields of privileged users or roles]. Individuals or roles with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Denying privileged access to further defined between audit-related privileges and other privileges, limits the number of users or roles with audit-related privileges.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-8 (4)</td>
<td>2</td>
<td>Audit and Accountability</td>
<td>Dual Authorization</td>
<td>[Assignment: organization-defined fields within audit records]. Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms (also known as two-person control) require the approval of two authorized individuals to execute audit functions. To reduce the risk of collusion, organizations consider rotating dual-authorization duties to other individuals. Organizations do not require dual-authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AU-I-9 (a) 2 Audit and Accountability | Protection of Audit Information | Readability Access

Provide audit trail-only access to audit information to assignment: organization-defined subset of privileged users or roles.

Restricting privileged user or role authorizations to read only helps to limit the potential damage to organizations that could be inflicted by such users or roles, for example, altering audit records to cover up malicious activity.

AU-I-9 (b) 2 Audit and Accountability | Protection of Audit Information | Store on Component with Different Operating System

Store audit information as a component running a different operating system than the system or component being audited.

Storing existing information on a system component running a different operating system reduces the risk of a vulnerability specific to the system resulting in a compromise of the audit records.

Related controls: AU-4, AU-5, AU-11, SI-20

AU-10 1 Audit and Accountability | Non-repudiation

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed (assignment: organization-defined actions to be covered by non-repudiation).

Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by users of not having authored certain documents, sender's of not transmitting messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual, or an individual link specific actions (e.g., sending an email, signing a contract, or approving a procurement request, or received specific information). Organizations obtain non-repudiation services by employing various technologies or mechanisms, including digital signatures and digital message receipts.

AU-10 (1) 2 Audit and Accountability | Non-repudiation | Validate

Audit and Accountability | Non-repudiation | Validate

AU-10 (2) 2 Audit and Accountability | Non-repudiation

Provide the means for authorized individuals to determine the identity of the producer of the information.

Binding identities to the information supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of attributes linking between the information producer and the information based on the security category of the information and other relevant risk factors.

AU-10 (3) 2 Audit and Accountability | Non-repudiation | Audit and Accountability | Audit Record Generation

Audit trails are time-correlated if the time stamps in the individual audit records can be correlated. Standard formats for audit records include audit records that can be readily analyzed and correlated. Standard formats for audit records include records that are compliant with Common Event Expressions. If logging mechanisms within a system are capable of maintaining audit records in a standardized format, they can be readily analyzed and correlated. Standard formats for audit records include records that are compliant with Common Event Expressions. If logging mechanisms within a system are capable of maintaining audit records in a standardized format, they can be readily analyzed and correlated.

AU-10 (4) 2 Audit and Accountability | Non-repudiation | Audit and Accountability | Audit Record Generation

Audit trails are time-correlated if the time stamps in the individual audit records can be correlated. Standard formats for audit records include audit records that can be readily analyzed and correlated. Standard formats for audit records include records that are compliant with Common Event Expressions. If logging mechanisms within a system are capable of maintaining audit records in a standardized format, they can be readily analyzed and correlated. Standard formats for audit records include records that are compliant with Common Event Expressions. If logging mechanisms within a system are capable of maintaining audit records in a standardized format, they can be readily analyzed and correlated.

AU-10 (5) 2 Audit and Accountability | Non-repudiation | Audit and Accountability | Audit Record Generation

Audit trails are time-correlated if the time stamps in the individual audit records can be correlated. Standard formats for audit records include audit records that can be readily analyzed and correlated. Standard formats for audit records include records that are compliant with Common Event Expressions. If logging mechanisms within a system are capable of maintaining audit records in a standardized format, they can be readily analyzed and correlated.

AU-11 1 Audit and Accountability | Audit Record Retention

Audit record retention requirements.

Records are needed for administrative, legal, audit, or other operational purposes. Retention of information is necessary to facilitate the retrieval of audit records, but without adequate controls, the potential exists for audit records to be altered or deleted.

Auditing the retention of information to facilitate the retrieval of data is a significant concern. Organizations develop standard categories of audit records relative to such types of actions and standard response measures for such types of actions. The National Archives and Records Administration (NARA) General Records Schedule provides federal policy on record retention.

AU-11 (1) 2 Audit and Accountability | Audit Record Retention | Long-term Retention Capability

Long-term retention of audit records is required to ensure that long-term audit records generated by the system can be retrieved.

Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to freedom of information (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response measures for such types of actions. The National Archives and Records Administration (NARA) General Records Schedule provides federal policy on record retention.

AU-11 (2) 2 Audit and Accountability | Audit Record Generation | System-wide and Time-bound Audit Trail

Audit trails on time-correlated if the time stamps in the individual audit records can be readily related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerance.

Audit trails on time-correlated if the time stamps in the individual audit records can be readily related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerance.

AU-11 (3) 2 Audit and Accountability | Audit Record Generation | Standardized Formats

Audit trails on time-correlated if the time stamps in the individual audit records can be readily related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerance.

Audit trails on time-correlated if the time stamps in the individual audit records can be readily related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerance.

AU-12 2 Audit and Accountability | Audit Record Generation | Changed by Authorized Individuals

Audit trails on time-correlated if the time stamps in the individual audit records can be readily related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerance.

Audit trails on time-correlated if the time stamps in the individual audit records can be readily related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerance.

AU-12 (1) 2 Audit and Accountability | Audit Record Generation | Query-Parameter Audits of Personally Identifiable Information

Audit trails on time-correlated if the time stamps in the individual audit records can be readily related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerance.

Audit trails on time-correlated if the time stamps in the individual audit records can be readily related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerance.

Notes

Withdrawn: incorporated into SI-7

Withdrawn: incorporated into SI-7

Withdrawn: incorporated into SI-7
AU-13 (2) Audit and Accountability | Monitoring for Information Disclosure | Use of Active Controls

Monitor open source information and information sites using [Assignment: organization-defined automated mechanism].

- Automated mechanisms include commercial services providing notifications and alert services to monitor new posts on websites.

AU-14 (1) Audit and Accountability | Session Audit | Monitoring for Information Disclosure | Unrestricted Replication of Information

- Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an uncontrolled manner.

- Uncontrolled use or replication of organizational information by external entities can cause adverse impact on organizational operations and assets, including damaging to reputation. Such activity can include, for example, the replication of an organizational website by an adversary or hostile threat actor who attempts to impersonate the web-based organization. Discovery tools and techniques must be sufficient to determine if external entities are replicating organizational information in an unauthorized manner, including scanning external websites, monitoring social media, and training staff to recognize unauthorized use of organizational information.

AU-14 (1) Audit and Accountability | Session Audit | System Start-up

- Monitor session audits automatically at system start-up.

- The initiation of session audits automatically at startup helps to ensure the information being captured on selected individuals is complete and is subject to comprehension through remedy by malicious threat actors.

AU-15 (1) Audit and Accountability | Alternate Audit Logging

- Provide and implement the capability for publicized users to remotely view and have control related to an established user session in real time.

- None.

AU-16 (1) Audit and Accountability | Cross-organizational Audit Logging

- Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

- When organizations use systems or services of external organizations, the audit logging capability includes a coordinated, cross-organization approach. For example, maintaining the identity of individuals that requested specific services across organizational boundaries may often be difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is the case that cross-organizational audit logging simply captures the identity of individuals issuing requests at the initial system, and subsequent systems record that the requests originated from authorized individuals. Organizations consider including procedures for coordinating audit information requirements and protection of audit information in information exchange agreements.

- None.

- AU-1, AU-4, AU-7, CA-3, FT-4

CA-1 Assessment, Authorization, and Monitoring

- Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
  - [Selection (one or more): organizational-level; mission/business process-level; system-level] assessment, authorization, and monitoring policy; and
  - [Assignment: organization-defined personnel or roles]; and
  - Two or more; if necessary, organization, operational, administrative, management, and personnel, and guidelines; and
  - Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls.

- This control addresses policy and procedures for the CA family implemented across systems and the organization. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the composite nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Remaining controls do not constitute an organizational policy or procedure.
LA-2 1 Assessment, Authorization, and Monitoring | Control Assessments
1. Develop a control assessment plan that describes the scope of the assessment including:
   a. Controls and control enhancements under assessment;
   b. Assessment procedures to be used to determine control effectiveness; and
   c. Assessment enrollment, assessment team, and assessment roles and responsibilities;
2. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
3. Assess the controls in the system and its environment of operation (assignment: organization-defined frequency) to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; and
4. Provide the results of the control assessment to (assignment: organization-defined individuals or roles).

LA-2 (1) 2 Assessment, Authorization, and Monitoring | Control Assessments | Independent Assessors
Display independent assessors or assessment teams to conduct control assessments.

LA-2 (2) 2 Assessment, Authorization, and Monitoring | Control Assessments | Specialized Assessments
Initiate as part of control assessments, (assignment: organization-defined frequency), (assignment: organization-defined frequency), (assignment: organization-defined frequency), (assignment: organization-defined frequency), and (assignment: organization-defined frequency), (assignment: organization-defined frequency), and (assignment: organization-defined frequency), (assignment: organization-defined frequency), (assignment: organization-defined frequency), and (assignment: organization-defined frequency), (assignment: organization-defined frequency).

LA-2 (3) 2 Assessment, Authorization, and Monitoring | Control Assessments | External Assessors
Assess the results of control assessments performed by (assignment: organization-defined external organization) or (assignment: organization-defined external organization) when the assessment meets (assignment: organization-defined external organization) or (assignment: organization-defined external organization) or (assignment: organization-defined external organization) or (assignment: organization-defined external organization) or (assignment: organization-defined external organization).

Notes
CA-3 | 1 | Assessment, Authorization, and Monitoring | Information Exchange

System information exchange requirements apply to information exchange between two or more systems. Security information exchanges include connections to local or virtual assets, connections to interconnection security agreements; information exchange security agreements, memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; and other agreements to assure coordination of actions.

X: Apprises and manages the exchange of information between the system and other systems. OR: Used for the exchange of information between the system and other systems. OR: Used for the system to communicate with other systems. OR: Used for the system to exchange information with other systems.

X: A plan of action and milestones for the system to document the planned remediation actions of the identified transitive (downstream) systems cannot be verified or validated.

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the identified transitive (downstream) systems.

To prevent unauthorized individual or systems from making information transfers to sensitive systems, the protocol system verifies via independent means, whether the individual or system attempting to transfer information is authorized to do so. This control enhancement also applies to control plane traffic (e.g., routing and DNS) and services such as automated SMTP relay.

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, and responsibilities for each system, and the impact level of the information exchanged.

Transitive or "downstream" information exchanges are information exchanges between the system and other systems that are external to the organization. A joint authorization of the systems exchanging information as described in CA-6(1) or CA-6(2) may help to communicate and reduce risk.

Current risk considerations include systems sharing the same assets, it is necessary to identify such information exchanges. The transparency of the connections to other systems is essential in understanding the security and privacy risks resulting from those interconnections. Organizational systems can inherit risk from systems that exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information as described in CA-6(1) or CA-6(2) may help to communicate and reduce risk.

CA-6(1) | 2 | Assessment, Authorization, and Monitoring | Information Exchange | Transitive Information Exchanges

To prevent unauthorized individual or systems from making information transfers to sensitive systems, the protocol system verifies via independent means, whether the individual or system attempting to transfer information is authorized to do so. This control enhancement also applies to control plane traffic (e.g., routing and DNS) and services such as automated SMTP relay.

X: Develop a plan of action and milestones for the system to document the planned remediation actions of the identified transitive (downstream) systems. OR: Used for the exchange of information between the system and other systems.

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, and responsibilities for each system, and the impact level of the information exchanged.

To prevent unauthorized individual or systems from making information transfers to sensitive systems, the protocol system verifies via independent means, whether the individual or system attempting to transfer information is authorized to do so. This control enhancement also applies to control plane traffic (e.g., routing and DNS) and services such as automated SMTP relay.

ca. Approve and manage the exchange of information between the system and other systems using [Selection: information exchange security agreements, [Selection: interconnection security agreements]. OR: Used for the exchange of information between the system and other systems.

b. Review and update the agreements [Assignment: organization-defined frequency]. OR: Used for the exchange of information between the system and other systems.

2. Plans of action and milestones are useful for any type of organization to track planned remediation actions. Plans of action and milestones are required in authorization packages and are subject to federal reporting requirements established by OMB.

b. Review and update the agreements [Assignment: organization-defined frequency]. OR: Used for the exchange of information between the system and other systems.

3. Planners and milestones are useful for any type of organization to track planned remediation actions. Plans of action and milestones are subject to federal reporting requirements established by OMB.
Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. Continuous monitoring at the system level involves, but is not limited to, the following system-level metrics to be monitored:

- Establishing the following system-level metrics to be monitored: (Assignment: organization-defined system-level metrics)
- Establishing (Assignment: organization-defined frequency) for monitoring and (Assignment: organization-defined frequency) for assessment of control effectiveness
- Ongoing control assessments in accordance with the continuous monitoring strategy
- Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy
- Correlation and analysis of information generated by control assessments and monitoring
- Reporting actions to address results of the analysis of control assessments and monitoring
- Reporting the security and privacy status of the system to (Assignment: organization-defined personnel or entity) (Assignment: organization-defined frequency)

A joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.

- Authorizations are official management decisions by senior officials to authorize operation of systems, to authorize the use of common controls for inheritance by organizational systems, and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing officials provide budgetary oversight for organizational systems and for common controls or assume responsibility for the mission and business operations supported by these systems or common controls. The authorization process is a federal responsibility and therefore, authorizing officials must be federal employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Federal-level organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Ongoing control assessments in accordance with the continuous monitoring strategy, the types of activities used in the continuous monitoring process need to be modified based on organizational systems; update the authorizations (Assignment: organization-defined frequency).

- Continuous monitoring supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, for example, AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, PE-5, PE-7a, PE-8, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-20, PM-14, PM-23, PM-31, PS-7a, SC-5(3)(b), SC-7a, SC-18, SC-38, SC-42, SC-43, SC-44, SI-1, SI-6, SI-18, SI-19, SI-20, SI-21, SI-22.

- Authorizations are withdrawn: Transmitted with CA-3(2)
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Document</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-7 [A]</td>
<td>2.3.1</td>
<td>Assessment, Authorization, and Monitoring</td>
<td>Continuous Monitoring</td>
<td>Risk Monitoring</td>
<td>[1] Monitor and manage an enterprise-level configuration management strategy that includes the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[a] Ensure that monitoring is an integral part of the continuous monitoring strategy that includes the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[b] Compliance monitoring; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[c] Change monitoring.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA-7 [A]</td>
<td>2.3.2</td>
<td>Assessment, Authorization, and Monitoring</td>
<td>Continuous Monitoring</td>
<td>Consistency Analysis</td>
<td>[1] Perform security and privacy compliance checks on constituent system components prior to the establishment of the system or system components.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA-8 [A]</td>
<td>2.3.3</td>
<td>Assessment, Authorization, and Monitoring</td>
<td>Penetration Testing</td>
<td>[1] Conduct penetration testing (Assignment: organization-defined frequency) on [Assignment: organization-defined systems or system components].</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA-8 [A]</td>
<td>2.3.4</td>
<td>Assessment, Authorization, and Monitoring</td>
<td>Penetration Testing</td>
<td>Real Team Exercises</td>
<td>[1] Conduct penetration testing that includes techniques, and procedures that are anticipated to be employed by adversaries.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA-9 [A]</td>
<td>2.3.5</td>
<td>Assessment, Authorization, and Monitoring</td>
<td>Internal System Connections</td>
<td>[1] Authorize internal connections to [Assignment: organization-defined systems or system components] to the system;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>a. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b. Terminate internal system connections after [Assignment: organization-defined conditions]; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>c. Review [Assignment: organization-defined frequency] the continued need for each internal connection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA-8 [A]</td>
<td>2.3.6</td>
<td>Assessment, Authorization, and Monitoring</td>
<td>Penetration Testing</td>
<td>[1] Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes**

- [Assignment: organization-defined systems or system components]
- [Assignment: organization-defined systems or system components]
- [Assignment: organization-defined systems or system components]
- [Assignment: organization-defined systems or system components]
- [Assignment: organization-defined systems or system components]
CM-1 1 Configuration Management | Policy and Procedures
a. Develop, document, and disseminate to [assignment: organization-defined personnel or roles]:
   i. Development, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   ii. To consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   b. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
   c. Designate an [assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
   d. Review and update the current configuration management plan.

This control addresses policies and procedures for the configuration controls in the CM family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are prioritized in general, and may dictate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Policies can be established for security and privacy programs for the systems, if needed. Procedures describe the policies or controls that are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in security and privacy plans or in one or more separate documents. Restricting controls does not constitute an organizational policy or procedure.

CM-2 1 Configuration Management | Baseline Configuration

CM-2(1) 2 Configuration Management | Baseline Configuration

CM-2(2) 2 Configuration Management | Baseline Configuration

CM-2(3) 2 Configuration Management | Baseline Configuration

CM-2(4) 2 Configuration Management | Baseline Configuration

CM-2(5) 2 Configuration Management | Baseline Configuration

CM-2(6) 2 Configuration Management | Baseline Configuration

CM-2(7) 2 Configuration Management | Baseline Configuration

Baseline configurations for systems and system components include connectivities, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed and agreed upon for systems or configuration items within those systems. Baseline configurations serve as a base for future builds, releases, or changes to systems and include security and privacy control: Implementations, operational procedures, information about system components, network mappings, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.

CM-2 1 Configuration Management | Baseline Configuration

CM-2(1) 2 Configuration Management | Baseline Configuration

CM-2(2) 2 Configuration Management | Baseline Configuration

CM-2(3) 2 Configuration Management | Baseline Configuration

CM-2(4) 2 Configuration Management | Baseline Configuration

CM-2(5) 2 Configuration Management | Baseline Configuration

CM-2(6) 2 Configuration Management | Baseline Configuration

CM-2(7) 2 Configuration Management | Baseline Configuration

Baseline configuration management provides a current baseline configuration of the system and:

a. Develop, document, and maintain under configuration control a current baseline configuration of the system; and
b. Review and update the baseline configuration of the system.

 retained previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, and configuration records.

CM-2(1) 2 Configuration Management | Baseline Configuration

CM-2(2) 2 Configuration Management | Baseline Configuration

CM-2(3) 2 Configuration Management | Baseline Configuration

CM-2(4) 2 Configuration Management | Baseline Configuration

CM-2(5) 2 Configuration Management | Baseline Configuration

CM-2(6) 2 Configuration Management | Baseline Configuration

CM-2(7) 2 Configuration Management | Baseline Configuration

Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configurations.

Establishing separate baseline configurations for development, testing, and operational environments protects systems from unplanned or unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, the management of operational configurations typically emphasizes the need for rapidity, while the management of development or test configurations requires greater flexibility. Configurations in the test environment mirror configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. Separate baseline configurations do not necessarily require separate physical environments.

CM-2(1) 2 Configuration Management | Baseline Configuration

CM-2(2) 2 Configuration Management | Baseline Configuration

CM-2(3) 2 Configuration Management | Baseline Configuration

CM-2(4) 2 Configuration Management | Baseline Configuration

CM-2(5) 2 Configuration Management | Baseline Configuration

CM-2(6) 2 Configuration Management | Baseline Configuration

CM-2(7) 2 Configuration Management | Baseline Configuration

Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including configurations, security, and privacy implementations, operational procedures, configuration change control systems; changes to operational environments; and changes to maintainability and supportability. Processes for managing configuration changes to systems include Configuration Management Boards or Change Advisory Boards that review and approve proposed changes. For changes impacting privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records representatives from the development organizations on the Configuration Control Boards.

When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations of areas that are of concern, defining the required configurations for the component, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specialized configured notebook computers include components with sanitized hard drives, limited applications, and zero configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and enabling strong authentication. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-3 (1)</td>
<td>2</td>
<td>Configuration Management</td>
<td></td>
<td>(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and (b) Automatically generate audit records of the enforcement actions.</td>
<td>Organizations log access records associated with applying configuration changes to ensure that configuration change control is implemented and to support the after-the-fact actions should organizations discover any unauthorized changes.</td>
<td>AU-1, AU-7, CM-5, SI-2</td>
<td></td>
</tr>
<tr>
<td>CM-3 (2)</td>
<td>2</td>
<td>Configuration Management</td>
<td></td>
<td>Test, validate, and document changes to the system before resolving the implementation of the changes.</td>
<td>Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-4. Organizations ensure that testing does not interfere with system operations supporting organizational missions and business functions. CIC-3 includes conducting tests under simulated and actual testing conditions, system security and privacy policies and procedures, and the health, safety, and environment risks associated with specific facilities or processes. Operational systems may need to be taken offline, or replicated to the external “sandbox,” before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outage whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.</td>
<td>AU-6, CM-2</td>
<td></td>
</tr>
<tr>
<td>CM-3 (3)</td>
<td>2</td>
<td>Configuration Management</td>
<td></td>
<td>Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined automated mechanisms].</td>
<td>Change controls refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components are certified for identification and authentication, a process is implemented to address the expiration of those certificates.</td>
<td>SA-11, SC-7</td>
<td></td>
</tr>
<tr>
<td>CM-3 (4)</td>
<td>2</td>
<td>Configuration Management</td>
<td></td>
<td>Automated security responses include: (a) validating and documenting changes to the system baseline across the installed base using [Assignment: organization-defined automated mechanisms]; and (b) implementing the current system baseline and deploying updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].</td>
<td>Automated tools (e.g., Security Information and Event Management tools) can improve the accuracy, consistency, and availability of configuration baseline information. Automation can also provide data aggregation and data correlation capabilities; starting mechanisms; and dashboards to support risk-based decision making within the organization.</td>
<td>SI-2, SI-12</td>
<td></td>
</tr>
<tr>
<td>CM-3 (5)</td>
<td>2</td>
<td>Configuration Management</td>
<td></td>
<td>Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined automated mechanisms] to determine whether unauthorized changes have occurred.</td>
<td>Organizations need to understand control implementation and how specific system changes might affect the requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing with stakeholders the impact of changes on organizational supply chain partners; and determining how potential changes to a system create new risks to the security and privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and to determine if additional controls are required.</td>
<td>SI-2, SI-12</td>
<td></td>
</tr>
<tr>
<td>CM-4 (1)</td>
<td>1</td>
<td>Configuration Management</td>
<td></td>
<td>Impact Analyses</td>
<td>Analysis changes to the system to determine potential security and privacy impacts prior to change implementation.</td>
<td>Impact Analyses change control elements define by organizations in CM-3. Automated tools (e.g., Security Information and Event Management tools) can improve the accuracy, consistency, and availability of configuration baseline information. Automation can also provide data aggregation and data correlation capabilities; starting mechanisms; and dashboards to support risk-based decision making within the organization.</td>
<td>CM-4, CM-5, CM-6, CM-7</td>
</tr>
<tr>
<td>CM-4 (2)</td>
<td>1</td>
<td>Configuration Management</td>
<td></td>
<td>Access Restrictions for Change</td>
<td>Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.</td>
<td>Access controls refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components are certified for identification and authentication, a process is implemented to address the expiration of those certificates.</td>
<td>SC-3, SA-11</td>
</tr>
<tr>
<td>CM-4 (3)</td>
<td>1</td>
<td>Configuration Management</td>
<td></td>
<td>Verification of Controls</td>
<td>After system changes, verify that the implemented controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.</td>
<td>Implementation in this context refers to installing changes to the operational system and may have an impact on security or privacy controls.</td>
<td>SI-2, SI-12</td>
</tr>
<tr>
<td>CM-4 (4)</td>
<td>1</td>
<td>Configuration Management</td>
<td></td>
<td>Impact Analyses</td>
<td>Analysis changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.</td>
<td>A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separating is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means.</td>
<td>SI-2, SI-12</td>
</tr>
<tr>
<td>CM-5 (1)</td>
<td>2</td>
<td>Configuration Management</td>
<td></td>
<td>Access Restrictions for Change</td>
<td>Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.</td>
<td>Access controls refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components are certified for identification and authentication, a process is implemented to address the expiration of those certificates.</td>
<td>AU-1, AU-7, CM-5, SI-2</td>
</tr>
</tbody>
</table>

Notes:
CM-5 (1) 1 Withdrawn: Incorporated into CM-1-17(2)
CM-3 (3) 2 Configuration Management | Access Restrictions for Change | System Configuration

**Control Text**

1. Establish and document configuration settings for components employed within the system using [Assignment: organization-defined common secure configurations] that reflect the most restrictive mode consistent with operational requirements.
2. Implement the configuration settings.
3. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
4. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

**Notes**

- Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include network computers, servers, workstations, operating systems, mobile devices, [Assignment: organization-defined device types, protocols, and/or services]. Security parameters are parameters impacting the security posture of systems, including the parameters required to satisfy other security control requirements. Security parameters include registry settings, account names, or directory permissions.

- Organizations establish organization-wide configuration settings and subsequently define specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

- Common secure configurations (also known as security configuration checklists, templates, and hardening guides, security reference guides) provide recognized, standardized, and established best practices that regulate secure configuration settings for information technology products and platforms as well as instructions for configuring these products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product vendors, manufacturers, vendors, federal agencies, academia, industry, and other organizations in the public and private sectors. Implementation of a common secure configuration may be mandated at the organizational level, mission/business process level, or system level, or may be mandated at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline (USGCB) and the security technical implementation guidance (STIG), which affect the implementation of CM-3 and other controls such as AC-10 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, test, and control configuration settings.
CM-7 (1) 2 Configuration Management / Least Functionality / Unclassified Software — Whitelisting
(b) Identify (assignment: organization-defined software programs authorized to execute on the system).
(i) Appropriate organization-defined software programs are not authorized to execute on the system.
(ii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(iii) Appropriate systems component inventories are maintained as part of component installations or removals, or during general system updates.
(iv) Appropriate systems component inventories are maintained as part of component installations.
(v) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(vi) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(vii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(viii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(ix) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(x) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xi) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xiii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xiv) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xv) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xvi) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xvii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xviii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xix) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xx) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.

CM-7 (2) 2 Configuration Management / Least Functionality / Accountability
(a) Appropriate organization-defined software programs are authorized to execute on the system.
(i) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(ii) Appropriate systems component inventories are maintained as part of component installations or removals, or during general system updates.
(iii) Appropriate systems component inventories are maintained as part of component installations.
(iv) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(v) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(vi) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(vii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(viii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(ix) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(x) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xi) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xiii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xiv) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xv) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xvi) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xvii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xviii) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xix) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.
(xx) Appropriate system component inventories are maintained as part of component installations, removals, or during general system updates.

CM-7 (3) 2 Configuration Management / Least Functionality / Automated Maintenance
(a) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(b) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(c) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(d) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(e) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(f) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(g) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(h) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(i) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(j) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(k) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(l) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(m) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(n) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(o) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(p) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(q) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(r) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(s) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(t) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(u) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(v) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(w) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(x) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(y) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(z) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.

CM-7 (4) 2 Configuration Management / Least Functionality / Automated Uncontrolled Component Detection
(a) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(b) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(c) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(d) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(e) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(f) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(g) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(h) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(i) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(j) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(k) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(l) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(m) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(n) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(o) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(p) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(q) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(r) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(s) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(t) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(u) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(v) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(w) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(x) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(y) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.
(z) Include in the system component inventory information, a means for identifying by (selection: true or false) of the software program.

CM-6 (1)
2 Configuration Management / System Component Inventory / Baseline Accounting of Components

(a) Verify that all components within the system are not duplicated in other system component inventories, or if a component is component inventory is valid, verify components are not assigned to multiple systems.

Preventing duplicate accounting of system components eliminates the risk of accountability that occurs where component ownership and system association is not known, especially in large or complex connected systems. For software inventory, centrally managed software that is accessed by other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system associated for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces. The implementation of CM-8(7) can help to eliminate duplicate accounting of components.

CM-9 (1)
2 Configuration Management / System Component Inventory / Authorized Configuration and Approved Deviations

Include assessed component configurations and any approved deviations to current deployed configuration in the system component inventory.

CM-8(7) can help to eliminate duplicate accounting of components.

CM-8 (2)
2 Configuration Management / System Component Inventory / Centralized Repository

Provide a centralized repository for the inventory of system components.

Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide assurance for efficiency in accounting for organizational hardware, software, and firmware assets. Such repositories also help organizations rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include specific information required for proper component accountability.

CM-8 (3)
2 Configuration Management / System Component Inventory / Automated Location Tracking

Support the tracking of system components by geographic location using [assignment: organization defined automation mechanisms].

The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. The use of tracking mechanisms can be controverted with senior agency officials for privacy if there are implications affecting individual privacy.

CM-9 (1)
2 Configuration Management / System Component Inventory / Assignment of Components to Systems

(a) Assign [assignment: organization defined required system component] to a system; and
(b) Describe an acknowledgment from [assignment: organization defined personnel or role] of this assignment.

Acquired system components that are not assigned to a specific system may be mismanaged, fail the required protection, and thus, become an organizational vulnerability. Organizations determine the types of system components that are subject to this control enhancement.

CM-9 (2)
2 Configuration Management / System Component Inventory / Assignment of Components to Systems

As such, there are developmental configuration management activities (e.g., the control of configuration management plans and procedures); it establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; it defines the configuration items for the system and places the configuration items under configuration management; it is reviewed and approved by [assignment: organization defined personnel or role]; and it protects the configuration management plan from unauthorized disclosure and modification.

Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of configuration management plans and procedures); it establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; it defines the configuration items for the system and places the configuration items under configuration management; it is reviewed and approved by [assignment: organization defined personnel or role]; and it protects the configuration management plan from unauthorized disclosure and modification.

CM-10 1 Configuration Management / Software Usage Restrictions

(a) Use software and associated documentation in accordance with contract agreements and copyright laws;
(b) Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
(c) Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.

Software license agreements that permit individuals to study, change, and improve the software license agreements that permit individuals to study, change, and improve the source code. However, remediating compromised, breached, or otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include specific information required for proper component accountability.

CM-10 (2)
2 Configuration Management / Software Usage Restrictions / Open Source Software

Establish the following restrictions on the use of open source software (assignment: organization defined restrictions).

Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are uniformly provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, remediating compromised, breached, or otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include specific information required for proper component accountability.

D-7
### CM-11 Configuration Management | User-installed Software

<table>
<thead>
<tr>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a. Isolate (Assignment: organization-defined policy) governing the installation of software by users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Enforce software installation policies through the following methods: (Assignment: organization-defined methods); and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Monitor policy compliance (Assignment: organization-defined frequency);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organizations-approved "app stores." Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

### CM-12 Configuration Management | Information Location

<table>
<thead>
<tr>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>a. Identify and document the location of (Assignment: organization-defined information) and the specific system components on which the information is processed and stored;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Document changes to the location (i.e., system or system component) where the information is processed and stored;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and the associated contingency planning controls;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and associated information reside in the system's component(s), and how information is being processed so that information flow can be understood, and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the system and the system component where the information resides (see FIPS 200). The location of the information and system component is also a factor in the architecture and design of the system (see SA-4, SA-6, SA-27).

### CP-0 Contingency Planning

<table>
<thead>
<tr>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a. Develop a contingency plan for the system that:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i. Identifies essential missions and business functions and associated contingency requirements;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ii. Identifies policies, procedures, and processes that address continuity and contingency management activities; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iii. Identifies and document the location of (Assignment: organization-defined information) and the specific system components on which the information is processed and stored;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iv. Addresses continuity and catastrophe plans regarding the covered data actions and the components that are identified as part of the system (see SC-16, SC-12, SA-27);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- This control addresses policy and procedures for the controls in the CP family implemented within an organization. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate in their development. Security and privacy program policies and procedures at the organizational level and statewide level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complete scope of the organization and procedures. Policies can be established for security and privacy programs for the systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Restating controls does not constitute an organizational policy or procedure.

### CP-1 Contingency Planning | Policy and Procedures

<table>
<thead>
<tr>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a. Develop, document, and disseminate to (Assignment: organization-defined personnel or roles):</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>i. (Selection of one or more: organization mission, mission/business process level, system level) contingency planning policy;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ii. Address policies, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iii. To be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iv. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Designate an [Assignment: organization-defined official] to manage the development, document, and dissemination of the contingency planning policy and procedures; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Review and update the current contingency planning policy;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Policy [Assignment: organization-defined frequency]; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. Procedures [Assignment: organization-defined frequency];</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information lifecycle which includes collection, generation, transformation, use, disclosure, retention, and disposal. A map of system data actions includes diverse data actions, elements of personally identifiable information being processed in the data actions, components of the system involved in the data actions, and the owners or operators of the components. Understanding what personally identifiable information is being processed (e.g., the sensitivity of the personally identifiable information), how personally identifiable information is being processed (e.g., if the data action is visible to the individual or is processed on the behalf of the system), and by whom (e.g., individuals may have different privacy preferences based on the entity that is processing the personally identifiable information) provides a number of contextual factors that are important to assessing the degree of privacy risk presented by the system. The data map may be an entry of any system design artifact that the organization is using. The development of this map may necessitate coordination between the privacy and security programs regarding the covered data actions and the components that are identified as part of the system.
Level 2: Contingency Planning

Contingency planning is a process that involves the development of plans and procedures to address potential disruptions to the operations of an organization. This document outlines the requirements for implementing contingency planning in an organization.

CP-2 (2) 2 Contingency Planning / Contingency Plan / Resume Missions and Business Functions

Plan for the resumption of selected essential missions and business functions within [assignment: organization-defined time period] of contingency plan activation.

Organizations may choose to conduct contingency planning activities to resume missions and business functions as part of business continuity planning or as part of business impact analysis. Organizations prioritize the resumption of missions and business functions. The time frame for the resumption of missions and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

CP-7 (1) 2 Contingency Planning / Contingency Plan / Capacity Planning

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

Contingency planning provides organizations with the ability to respond to environmental changes and prepare for potential vulnerabilities. This includes strategies for staff training and communications with governmental agencies and other organizations.

CP-8 (1) 2 Contingency Planning / Contingency Plan / Critical System Assets

Identify critical system assets within or supported by external service providers. Critical system assets are resident within or supported by external service providers, organizations consider operational aspects including procedures (manually executed operations) and personnel (specific to contingency planning).

Organizations may choose to conduct contingency planning activities to continue missions and business functions at alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity until system restoration at primary processing and/or storage sites.

CP-9 (1) 2 Contingency Planning / Contingency Plan / Critical Information

Protect critical information assets against threats such as loss of data.

Critical information assets within organizations include system components, information technology resources, and personnel. Operational aspects include procedures (manually executed operations) and personnel (specific to contingency planning).

CP-10 (1) 2 Contingency Planning / Contingency Plan / Environmental Support

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and support services intended to support essential missions and business functions is available.

Capacity planning is a complex activity that can result in a reduction of the available processing, telecommunications, and support services intended to support essential missions and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if it is a degraded state. Such determinations are based on an organizational assessment of the system configuration (impact level), and organizational risk tolerance.

Notes

Withdrawn: Incorporated into CP-2 (3)

Withdrawn: Incorporated into CP-2 (3)

Withdrawn: Incorporated into CP-2 (3)

Page 31 of 108

OIGOM Control Set for NIST SP 800-53 rev. 5 Final Public Draft

Page 31 of 108

OIGOM Control Set for NIST SP 800-53 rev. 5 Final Public Draft
CP-4 (3) 2 Contingency Planning | Contingency Plan Testing | Automated Testing  [Updated: organization-defined automated mechanisms]  Automated mechanisms facilitate thorough and effective testing of contingency plans by providing more complete coverage of contingency issues, by testing more realistic test scenarios and environments; and by effectively stressing the system and supporting missions and business operations.

CP-4 (4) 2 Contingency Planning | Contingency Plan Testing | Full Recovery and Reconstitution  Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing. Recovery is executing contingency plan activities to recover organizational missions and business functions. Reconstitution takes place following recovery and includes activities for returning systems to a fully operational state. Organizations establish a known state for systems that includes system state information for hardware, software programs, and data. Reconstitution may establish a new state for operational use or return to an operational mode with less disruption of mission and business processes.

CP-5 1 Contingency Planning | Contingency Plan Update  X

CP-6 1 Contingency Planning | Alternate Storage Site

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and
b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Alternate storage sites are sites that are geographically distinct from primary storage sites and that maintain duplicate copies of information and data in the primary storage site is not available. In contrast to alternate storage sites, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may also be considered as alternate storage sites. Terms covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions and business functions despite disruptions, compromise, or failure in organizational systems.

CP-6 (1) 2 Contingency Planning | Alternate Storage Site | Separation from Primary Site  Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors or omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

CP-6 (2) 2 Contingency Planning | Alternate Storage Site | Recovery Time and Recovery Point Objectives  Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations ensuring accessibility and correct execution.

CP-6 (3) 2 Contingency Planning | Alternate Storage Site | Accessibility  Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Area-wide disruptions refer to those types of disruptions that are widespread in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur or uniquely designated alternate sites; or planning for physical access to retrieve backup information electronically if accessibility to the alternate site is disrupted.

CP-7 1 Contingency Planning | Alternate Processing Site

a. Establish an alternate processing site, including necessary agreements to permit the transfer and reception of (assignment: organization-defined system operating) for essential missions and business functions within organizations. Geographically distributed time-period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable;
b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery of the site within the organization-defined time-period for transfer and resumption; and
c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Alternate processing sites are sites that are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives such as a cloud-based service provider or other internal or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered as alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental condition at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions and business functions despite disruptions, compromise, or failure in organizational systems.

CP-7 (1) 2 Contingency Planning | Alternate Processing Site | Separation from Primary Site  Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors or omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

CP-7 (2) 2 Contingency Planning | Alternate Processing Site | Priority of Service  Develop alternate processing site agreements that contain priority of service provisions in accordance with availability requirements (including recovery time objective).

Priority of service agreements refer to negotiated agreements between service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

CP-7 (3) 2 Contingency Planning | Alternate Processing Site | Preparation for Use  Prepare the alternate processing site so that the site can serve in the operational site supporting essential missions and business functions.

Site preparation includes: establishing configuration settings for systems of the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.

CP-7 (4) 2 Contingency Planning | Alternate Processing Site | Inability to Return to Primary Site  Plan and prepare for circumstances that preclude returning to the primary processing site.

There may be situations that preclude an organization from returning to the primary processing site. This can occur, for example, if a natural disaster such as a flood or a hurricane damaged or destroyed a facility and it was determined that rebuilding in the same location was not prudent.

CP-8 1 Contingency Planning | Telecommunications Services

Establish alternate telecommunications services, including necessary agreements to permit the reception of (assignment: organization-defined system operating) for essential missions and business functions within organizations. Geographically distributed time-period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

This control applies to telecommunications services for data and video for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions and business functions despite the loss of primary telecommunications services. Organizations may specify different time-periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines or the use of satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Document</th>
<th>Remaining Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-9 (1)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Conduct backups of user-level information contained in [Assignment: organization-defined system]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparations if the primary and alternate telecommunications services are provided by a common carrier.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Organizations consider the potential mission-critical impact in situations where telecommunications services providers are serving other organizations with similar priority of service providers. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that affects telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to ensure the continued existence of the program when they want to add new lines of similar high value or their lines must follow a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or other taking place. Federal sponsorship is required to enroll in the TSP program.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (2)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>In certain circumstances, telecommunications services providers or services may share the same physical lines, which increases the vulnerability of a single point failure. It is important to have provider transparency for the actual physical transmission capability for telecommunications services.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (3)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Obtain alternate telecommunications services from providers that are separated from primary service provider to reduce susceptibility to the same threats.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Documents that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical intrusions, and errors of omission or commission. Organizations can use external redundancies by extending shared infrastructure among telecommunications service providers and achieve sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (4)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Obtain primary and alternate telecommunications services to have contingency plans;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. Review provider contingency plans to ensure that the plans meet organizational contingency requirements;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3. Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency].</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy contingency-related requirements to provider service contingency plans.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (5)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Test secondary telecommunication service testing arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure there is no degradation in organizational missions or functions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (6)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Conduct backups of over-level information contained in [Assignment: organization-defined system components]. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3. Conduct backups of system documentation, including security and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4. Protect the confidentiality, integrity, and availability of backup information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of backup information while in transit is outside the scope of this control. System backups reflect the requirements in contingency plans as well as other organizational requirements for testing backup information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (7)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Organizations need assurance that backup information can be reliably retrieved. Retrievability pertains to the systems and systems components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specified test can be used for each of the aspects of retrievability, for example, datacopying and non-replicating (removing) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (8)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Test restoration using backup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is used to determine if the functions operate as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (9)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Separate storage for critical information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Store backup copies of assignment: organization-defined critical system software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the operational system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating system, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may provide separate storage by implementing automated backup processes or alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire-rated containers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-9 (10)</td>
<td>2</td>
<td>Contingency Planning / Telecommunications Services</td>
<td></td>
<td>1. Ensure dual authorization for the detection or obstruction of [Assignment: organization-defined backup information].</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dual authorization ensures that deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting or destroying backup information possess the skills or expertise to determine if the proposed deletion or obstruction of information reflects organizational policies and procedures. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control ID</td>
<td>Level</td>
<td>Control Name</td>
<td>Withdrawn</td>
<td>Control Text</td>
<td>Discussion</td>
<td>Related Controls</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>--------------</td>
<td>-----------</td>
<td>--------------</td>
<td>------------</td>
<td>-----------------</td>
<td>-------</td>
</tr>
<tr>
<td>CP-8 (3)</td>
<td>2</td>
<td>Contingency Planning</td>
<td>System Recovery</td>
<td>System Backup</td>
<td>Implement cryptographic mechanism to prevent unauthorized disclosure and modification of (assignment: organization-defined backup information);</td>
<td>The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. The control environment applies to system backup information in storage of primary and alternate locations. Organizations implementing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.</td>
<td>D-12, I-10, I-28</td>
</tr>
<tr>
<td>CP-10 (1)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>System Recovery and Reconstitution</td>
<td>Provide for the recovery and reconstitution of the system to an acceptable state within (assignment: organization-defined period consistent with recovery time and recovery point objectives) after a disruption, compromise, or failure.</td>
<td>Recovery is executing contingency plan activities to restore organizational missions and business functions. Reconstitution takes place following recovery and includes activities for restoring systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point, recovery time, and reconstitution objectives, and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, restoration of continuous monitoring activities, system hardenization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.</td>
<td>CP-2, CP-4, CP-6, CP-7, CP-9, IA-4, SA-6, SC-24, SI-13</td>
<td></td>
</tr>
<tr>
<td>CP-10 (2)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>System Recovery and Reconstitution</td>
<td>Contingency Plan Testing</td>
<td>Implement transaction recovery for systems that are transaction-based.</td>
<td>Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.</td>
<td>X</td>
</tr>
<tr>
<td>CP-10 (3)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>System Recovery and Reconstitution</td>
<td>Transaction Testing</td>
<td>Implement transaction recovery for systems that are transaction-based.</td>
<td>Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.</td>
<td>Addressed through training procedures.</td>
</tr>
<tr>
<td>CP-10 (4)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>System Recovery and Reconstitution</td>
<td>System Recovery and Reconstitution</td>
<td>Implement transaction recovery for systems that are transaction-based.</td>
<td>Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.</td>
<td>X</td>
</tr>
<tr>
<td>CP-10 (5)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>System Recovery and Reconstitution</td>
<td>System Recovery and Reconstitution</td>
<td>Implement transaction recovery for systems that are transaction-based.</td>
<td>Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.</td>
<td>X</td>
</tr>
<tr>
<td>CP-11 (1)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>Alternate Communications Protocols</td>
<td>Protect system components used for recovery and reconstitution.</td>
<td>Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilations, and other system software.</td>
<td>OA-1, OA-6, MP-2, MP-4, PE-3, PE-6</td>
<td></td>
</tr>
<tr>
<td>CP-11 (2)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>Alternate Communications Protocols</td>
<td>Protect system components used for recovery and reconstitution.</td>
<td>Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilations, and other system software.</td>
<td>OA-1, OA-6, MP-2, MP-4, PE-3, PE-6</td>
<td></td>
</tr>
<tr>
<td>CP-11 (3)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>Alternate Communications Protocols</td>
<td>Protect system components used for recovery and reconstitution.</td>
<td>Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilations, and other system software.</td>
<td>OA-1, OA-6, MP-2, MP-4, PE-3, PE-6</td>
<td></td>
</tr>
<tr>
<td>CP-12 (1)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>Alternate Communications Protocols</td>
<td>Protect system components used for recovery and reconstitution.</td>
<td>Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilations, and other system software.</td>
<td>OA-1, OA-6, MP-2, MP-4, PE-3, PE-6</td>
<td></td>
</tr>
<tr>
<td>CP-13 (1)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>Alternate Communications Protocols</td>
<td>Protect system components used for recovery and reconstitution.</td>
<td>Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilations, and other system software.</td>
<td>OA-1, OA-6, MP-2, MP-4, PE-3, PE-6</td>
<td></td>
</tr>
<tr>
<td>CP-13 (2)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>Alternate Communications Protocols</td>
<td>Protect system components used for recovery and reconstitution.</td>
<td>Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilations, and other system software.</td>
<td>OA-1, OA-6, MP-2, MP-4, PE-3, PE-6</td>
<td></td>
</tr>
<tr>
<td>CP-14 (1)</td>
<td>1</td>
<td>Contingency Planning</td>
<td>Alternate Communications Protocols</td>
<td>Protect system components used for recovery and reconstitution.</td>
<td>Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilations, and other system software.</td>
<td>OA-1, OA-6, MP-2, MP-4, PE-3, PE-6</td>
<td></td>
</tr>
<tr>
<td>IA-1 (1)</td>
<td>1</td>
<td>Identification and Authorization</td>
<td>Policy and Procedures</td>
<td>Policy (assignment: organization-defined personnel or roles);</td>
<td>This control addresses policy and procedures for the identification and authorization of personnel or roles within an organization. The control environment applies to systems implementing policies and procedures for granting access to system resources and services. Organizations implementing policies and procedures for identification and authorization focus on ensuring that the control environment is in place to support the objectives of the organization.</td>
<td>AC-1, PA4-6, SI-13</td>
<td></td>
</tr>
<tr>
<td>IA-1 (2)</td>
<td>1</td>
<td>Identification and Authorization</td>
<td>Policy and Procedures</td>
<td>Procedures (assignment: organization-defined personnel or roles);</td>
<td>This control addresses policy and procedures for the identification and authorization of personnel or roles within an organization. The control environment applies to systems implementing policies and procedures for granting access to system resources and services. Organizations implementing policies and procedures for identification and authorization focus on ensuring that the control environment is in place to support the objectives of the organization.</td>
<td>AC-1, PA4-6, SI-13</td>
<td></td>
</tr>
</tbody>
</table>

Page 34 of 108
### Level 1 - Identification and Authentication (Organizational Users)

<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-2 (1)</td>
<td>1</td>
<td>Identification and Authentication (Organizational Users)</td>
<td>Yes</td>
<td>(uniquely) identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.</td>
</tr>
</tbody>
</table>

Organizations can satisfy the identification and authentication requirements by complying with the requirements in (HSPD 12). Organizational users include employees or individuals that organizations consider having equivalent status of employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than accesses that are explicitly accounted for in AC-16 and that occur through the authorized use of group authenticators without individual authentication. Since processes acting on behalf of groups and roles, organizations may require unique identification of individual group accounts or for detailed accountability of individual activity. Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users or processes acting on behalf of users, where access is obtained through network connections (i.e., nonlocal access). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-6.

#### AC-2 (1)

2 | Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts | Implement multi-factor authentication for access to privileged accounts. |

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number (PIN)); something you have (e.g., a physical authenticator or an cryptographic private key stored in hardware or software); something you are (e.g., a biometric). Multi-factor authentication solutions also feature physical authenticators include hardware authenticators providing time-based or challenge-response authentication and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level (i.e., at login), organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (e.g., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

#### AC-2 (2)

2 | Identification and Authentication (Organizational Users) | Multi-factor Authentication to Non-privileged Accounts | Implement multi-factor authentication for access to non-privileged accounts. |

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number (PIN)); something you have (e.g., a physical authenticator or an cryptographic private key stored in hardware or software); or something you are (e.g., a biometric). Multi-factor authentication solutions also feature physical authenticators include hardware authenticators providing time-based or challenge-response authentication and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level (i.e., at login), organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access, non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

#### AC-3 (1)

2 | Identification and Authentication (Organizational Users) | Limit Access to Non-privileged Accounts | X | Withdrawn: Incorporated into IA-2 (1). |

#### AC-3 (2)

2 | Identification and Authentication (Organizational Users) | Limit Access to Non-privileged Accounts | X | Withdrawn: Incorporated into IA-2 (2). |

#### AC-3 (3)

2 | Identification and Authentication (Organizational Users) | Group Authentication with Group Authorization | Where channel accounts or authenticators are employed, require users to be individually authenticated before gaining access to the shared accounts or resources. |

Individual authentication prior to shared group authentication helps to mitigate the risk of unauthorized access to shared accounts or resources.

#### AC-3 (4)

2 | Identification and Authentication (Organizational Users) | Access to Accounts — Separate Device | Implement multi-factor authentication for (selective (one or more) level; network; remote) access to (selective (one or more) privileged accounts; non-privileged accounts) such that: [a] One of the factors is provided by a device separate from the system gaining access; and [b] The device meets (assignment: organizational level strength of mechanism requirement). |

The purpose of requiring a device that is separate from the system is to which the user is attempting to gain access for one of the factors during multi-factor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. Adversaries may be able to compromise credentials stored on the system and subsequently impersonate authorized users. Implementing one of the factors in multi-factor authentication (e.g., a hardware token) as a separate device, provides a greater strength of mechanism and an increased level of assurance in the authentication process.

#### AC-3 (5)

2 | Identification and Authentication (Organizational Users) | Access to Accounts — Appply Resistant | Implement replay-resistant authentication mechanisms for access to (selective (one or more) privileged accounts; non-privileged accounts). |

Authentication processes must employ techniques (e.g., imposing) to achieve successful authentication by employing previous authentication messages. Replay-resistant techniques include protocols that use counter or challenges such as time-synchronous or challenge-response one-time time authentication.

#### AC-3 (6)

2 | Identification and Authentication (Organizational Users) | Network Access to Non-privileged Accounts — Replay Resistant | X | Withdrawn: Incorporated into IA-2 (8). |
Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.

Provide a single sign-on capability for (assignment: organization-defined systems and services).

Accept and electronically verify personal identity verification credential standards.

Implement the following out-of-band authentication mechanisms under (assignment: organization-defined conditions): (assignment: organization-defined out-of-band authentication).

Uniquely identify and authenticate (assignment: organization-defined devices and/or types of devices) before establishing a connection (one or more): local, remote, network connection.

Manage system identifiers by: a. Receiving authorization from (assignment: organization-defined personnel or roles) to assign an individual, group, role, service, or device identifier; b. Assigning the identifier to the intended individual, group, role, service, or device; and c. Preventing the reuse of identifiers implies preventing the assignment of previously used individual identifiers not necessarily associated with system accounts.
IA-4: (5) Identification and Authentication | Authenticator

The requirement for organizations to change default authenticators upon system initialization extends to the requirement for organizations to change default authenticators upon system initialization. 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 RA-4 or RA-5 for authenticators in the possession of individuals and organizational systems, including authenticators stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed re-uses during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

IA-5: Identification and Authentication | Authenticator Management

Protect authenticators commensurate with the security category of the information to which use of the authenticator is permitted. Characteristics identifying the status of individuals include contractors and foreign nationals. Identifying the status of individuals by characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that the user of an email message is a contractor.

IA-6: (4) Identification and Authentication | Authenticator Management

Changing authenticators prior to delivery and installation of system components extends the requirement for organizations to change default authenticators upon system installation, by requiring developers and/or installers to provide unique authentication or change default authenticators for system components prior to delivery and/or installation. However, if this practice applies to developers of commercial off-the-shelf information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when processing systems or system components.

Notes

Withdrawn: Incorporated into IA-12 (4)
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Revised Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-5 (4)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>Implement (assignment: organization-defined security controls) to manage the risk of compromise due to individuals having accounts on multiple systems.</td>
<td>When individuals have accounts on multiple systems, there is the risk that a compromise of one account may lead to the compromise of other accounts. If individuals use the same authenticators, Alternatives include having different authenticators on all systems, employing a single sign-on mechanism, or using some form of one-time passwords on all systems. Organisations can also use one of behavior (see Ps-4) and access agreements (see Ps-6) to mitigate the risk of multiple system accounts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IA-5 (6)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>Use the following external organizations to facilitate authentications: (assignment: organization-defined external organizations)</td>
<td>Federation provides the capability for organisations to authenticate individuals and devices when conducting cross-organisation activities involving the processing, storage, or transmission of information.</td>
<td>Au-7, Au-15, Au-16</td>
<td></td>
</tr>
<tr>
<td>IA-5 (10)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>Authenticator feedback from systems does not provide information that would allow the identity after authentication. In these situations, organisations can anticipate the dynamic provisioning of identities. Pre-established trustworthiness and mechanisms with appropriate authorities to validate identities and related credentials are essential.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IA-5 (12)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>For biometric-based authentication, employ presentation attack detection mechanisms for biometric-based authentication. Biometric characteristics do not constitute secrets. Such characteristics can be obtained by</td>
<td>Presentation attack detection technologies including liveness detection, can serve as the basis of comparison. Matching performance is the rate at which a biometric algorithm correctly matches a genuine user and rejects other users. Biometric performance requirements include the match rate as this rate reflects the accuracy of the biometric matching algorithm used by a system.</td>
<td>AC-7</td>
<td></td>
</tr>
<tr>
<td>IA-5 (13)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>For PS-6) to mitigate the risk of multiple system accounts.</td>
<td>Alternatives include having different authenticators on all systems, employing a single sign-on mechanism, or using some form of one-time passwords on all systems. Organisations can also use one of behavior (see Ps-4) and access agreements (see Ps-6) to mitigate the risk of multiple system accounts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IA-5 (14)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>For biometric-based authentication, employ presentation attack detection mechanisms for biometric-based authentication. Biometric characteristics do not constitute secrets. Such characteristics can be obtained by</td>
<td>Presentation attack detection technologies including liveness detection, can serve as the basis of comparison. Matching performance is the rate at which a biometric algorithm correctly matches a genuine user and rejects other users. Biometric performance requirements include the match rate as this rate reflects the accuracy of the biometric matching algorithm used by a system.</td>
<td>AC-7</td>
<td></td>
</tr>
<tr>
<td>IA-5 (15)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>For biometric-based authentication, employ presentation attack detection mechanisms for biometric-based authentication. Biometric characteristics do not constitute secrets. Such characteristics can be obtained by</td>
<td>Presentation attack detection technologies including liveness detection, can serve as the basis of comparison. Matching performance is the rate at which a biometric algorithm correctly matches a genuine user and rejects other users. Biometric performance requirements include the match rate as this rate reflects the accuracy of the biometric matching algorithm used by a system.</td>
<td>AC-7</td>
<td></td>
</tr>
<tr>
<td>IA-5 (16)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>For biometric-based authentication, employ presentation attack detection mechanisms for biometric-based authentication. Biometric characteristics do not constitute secrets. Such characteristics can be obtained by</td>
<td>Presentation attack detection technologies including liveness detection, can serve as the basis of comparison. Matching performance is the rate at which a biometric algorithm correctly matches a genuine user and rejects other users. Biometric performance requirements include the match rate as this rate reflects the accuracy of the biometric matching algorithm used by a system.</td>
<td>AC-7</td>
<td></td>
</tr>
<tr>
<td>IA-5 (17)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td></td>
<td>Ensure that the issuance of (assignment: organization-defined types of and/or specific authenticators be conducted (in the interest of) by a trusted external party) in order to manage the risk of compromise of the identity after authentication. In these situations, organisations can anticipate the dynamic provisioning of identities. Pre-established trustworthiness and mechanisms with appropriate authorities to validate identities and related credentials are essential.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IA-6</td>
<td>1</td>
<td>Identification and Authentication</td>
<td></td>
<td>Disclose feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.</td>
<td>Authenticator feedback from systems does not provide information that would allow unauthorised individuals to compromise authentication mechanisms. For some types of systems, for example, desktops or notebooks with relatively large monitors, the threat referred to as shoulder surfing may be significant. For other types of systems, for example, mobile devices with small displays, the threat may be less significant, and is balanced against the increased likelihood of topological input errors due to small displays. Thus, the means for obscuring authenticator feedback is selected accordingly. Disclosing authenticator feedback includes displaying entwined when enter type passwords into input devices, or displaying feedback for a very limited time before obscuring it.</td>
<td>AC-3</td>
<td></td>
</tr>
<tr>
<td>IA-7</td>
<td>1</td>
<td>Identification and Authentication</td>
<td></td>
<td>Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.</td>
<td>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.</td>
<td>AC-1, AC-5, AC-6, AC-12, AC-13</td>
<td></td>
</tr>
</tbody>
</table>
AIA-8 1 Identification and Authentication | Identification and
Authentication (non-organizational users) Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Non-organizational users include system users other than organizational users explicitly approved by Level 3. Non-organizational users are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-10. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors, including security, privacy, scalability, and practicality in balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

AIA-8 (1) 2 Identification and Authentication | Identification and
Authentication (non-organizational users) | Acceptance of PIV Credentials from Other Agencies
Accept and electronically verify personal identity verification compliant credentials from other federal agencies.

Acceptance of personal identity verification (PIV) credentials from other federal agencies is required to both logical and physical access control systems. PIV credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidelines. The adequacy and reliability of PIV card issuers are addressed and authorized using SP 800-79-2.

AIA-8 (2) 2 Identification and Authentication | Identification and
Authentication (non-organizational users) | Acceptance of PIV Credentials
Accept only electronic credentials that are PIV-compliant.

Acceptance of only PIV-compliant electronic credentials applies to organizational systems that are accessible to the public (e.g., public-facing websites). External credentials are those credentials issued by non-federal government entities. External credentials are certified as compliant with SP 800-63-3 by an approved accreditation authority. Approved external credentials meet the net of minimum federal government wide technical, security, privacy, and organizational security requirements. Meeting or exceeding federal requirements allow federal government relying parties to trust external credentials at their approved assurance levels.

AIA-8 (3) 2 Identification and Authentication | Identification and
Authentication (non-organizational users) | Use of Pre-approved Products
Use of FICAM-pre-approved products.

AIA-8 (4) 2 Identification and Authentication | Identification and
Authentication (non-organizational Users) | Use of Non-issued Profiles
Conform to NIST issued profiles for identity management.

Confirms with NIST issued profiles for identity management addresses open identity management standards. To ensure that open identity management standards are viable, robust, scalable, sustainable, and interoperable as documented, the United States Government assesses and adopts the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. The result is NIST issued implementation profiles of approved protocols.

AIA-8 (5) 2 Identification and Authentication | Identification and
Authentication (non-organizational users) | Acceptance of PIV Credentials
Accept and verify (federated or PIV) credentials that meet the organization-defined policy.

This control enhancement can be implemented by PIV, PIV-I, and other common or external identity providers. Authentication and verification of personal identity verification (PIV)-compliant credentials applies to both logical and physical access control systems. Acceptance and verification of PIV credentials addresses non-federal issues of identity that does not use to operate with United States Government PIV systems and that can be required by federal government relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV requirements. The PIV-I is a certificate with the PIV card as defined in the references. PIV-I credentials are the credentials issued by a PIV provider whose PIV-I certificate policy maps to the Federal Bridge Certification Policy. A PIV-I card is cross-certified with the Certificate Authority (FCA) and through another PIV bridge (or path) with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FCA certificate policy.

AIA-8 (6) 2 Identification and Authentication | Identification and
Authentication (non-organizational users) | Disassociability
Implement the following measures to disassociate user attributes or credential entities relationships among individuals, credential service providers, and relying parties (assignment: organization-defined measures).

Disassociability activities can create increased privacy risks due to tracking and profiling of individuals. Using identifier mapping tables or incapable techniques to link credential service providers and relying parties from each other or to identify entities into assess to misusing parties can reduce these privacy risks.

AIA-9 1 Identification and Authentication | Service Identification and Authentication
Uniquely identify and authenticate (assignment/organization defined) system services and applications (also identify establishing communications with devices, users, or other services or applications).

Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database. Identification and authentication methods for system services/applications include information or code signing, provenance graphs, and electronic signatures indicating the sources of services. Organizations regarding the validation of identification and authentication claims can be made by services separate from the services using on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication decisions (instead of actual identifiers and authentication) are provided to the services that need to act on those decisions.

AIA-9 (1) 2 Identification and Authentication | Service Identification and Authentication | Information Exchange
Implement decisions.

AIA-9 (2) 2 Identification and Authentication | Service Identification and Authentication | Transmission of Decisions
Implement decisions.

AIA-10 1 Identification and Authentication | Adaptive
Authentication
Require individuals accessing the system to employ (assignment: organization-defined supplemental authentication techniques/mechanisms) under specific (assignment: organization-defined circumstances or situations).

Adaptive authentication may incorporate individual authentication mechanisms employed by organizations and subsequently attempt to incorporate legitimate users. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behavior. Suspicious behavior may include accessing information that individuals do not typically access as part of their duties, roles, or responsibilities; accessing greater quantity of information than individuals would normally access, or attempting to access information from suspicious network addresses. When pre-established conditions or trigger occur, organizations can require individuals to provide additional authentication information. Another potential use for adaptive authentication is to increase the strength of mechanism based on the number of types of records being accessed. Adaptive authentication does not replace and is not used to avoid the use of multilateral authentication mechanisms but can augment implementations of these controls.

AIA-11 1 Identification and Authentication | Re-authentication
Require users to re-authenticate when (assignment: organization-defined circumstances or situations requiring re-authentication).

In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when authentication or roles change; when security categories of systems change; when the execution of privileged functions occurs; after a fixed time period; or periodically.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-2</td>
<td>1</td>
<td>Identification and Authentication</td>
<td>Identity Proofing</td>
<td>a. Identify proof users that require access to logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence.</td>
<td>Identity proofing is the process of validating, verifying, and verifying user identity information for the purposes of granting access to systems. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include (SP 800-63-4) and (SP 800-50).</td>
</tr>
<tr>
<td>IA-21 (1)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td>Incident Response</td>
<td>Require that the registration process to receive an account for logical access includes supervisor or sponsor authentication.</td>
<td>Including supervisor or sponsor authentication as part of the registration process provides an additional level of scrutiny to ensure that the user’s management level is aware of the account, the account is essential to carry out organizational missions and functions, and the user’s privileges are appropriate for the anticipated responsibilities and authorities within the organization.</td>
</tr>
<tr>
<td>IA-21 (2)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td>Incident Response</td>
<td>Require evidence of individual identification be presented to the registration authority.</td>
<td>Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risk to the system, role, and privilege associated with the user's account.</td>
</tr>
<tr>
<td>IA-21 (3)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td>Incident Response</td>
<td>Require that the presented identity evidence be validated and verified through (Assignment: organization-defined methods of validation and verifications); Winkling and verifying identity evidence increases the assurance that accounts, identities, and authorizations are being issued to the correct user. Validation reduces the process of confirming that the evidence is genuine and authoritative, and the data contained in the evidence is current, correct, and relevant to an actual person or individual. Verification confirms and establishes a linkage between the claimed identity and the actual evidence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risk to the system, role, and privileges associated with the user's account.</td>
<td></td>
</tr>
<tr>
<td>IA-21 (4)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td>Incident Response</td>
<td>Require that the validation and verifications of identity evidence be conducted in a person before a designated registration authority.</td>
<td>In person proofing reduces the likelihood of fraudulent identification being caused because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.</td>
</tr>
<tr>
<td>IA-21 (5)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td>Incident Response</td>
<td>Require that the selected registration center, center of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record.</td>
<td>To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to increase assurance that the individual associated with an address of record is the same person that participated in the registration. Confirmation can take the form of a temporary enrollment code or a center of proofing. The delivery addresses for these artifacts are obtained from records and not self-assessed by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.</td>
</tr>
<tr>
<td>IA-21 (6)</td>
<td>2</td>
<td>Identification and Authentication</td>
<td>Incident Response</td>
<td>Accept externally-proofed identities or (Assignment: organization-defined identity assurance level); To limit unnecessary re-proofing of identities, particularly of non-PIV users, organizations accept proofing conducted at a commensurate level of assurance by other agencies or organizations. Proofing is consistent with organizational security policy and with the identity assurance level appropriate for the system, application, or information accessed. Accepting externally-proofed identities is a fundamental component of managing identified identities across agencies and organizations.</td>
<td></td>
</tr>
<tr>
<td>IR-0</td>
<td>1</td>
<td>Incident Response</td>
<td>Policy and Procedures</td>
<td>a. Develop, document, and disseminate to (Assignment: organization-defined personnel or roles); b. Selective (one or more): organization-level, mission/business process level, system-level incident response policy and procedures; c. Address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and d. Be consistent with applicable laws, execute orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; d. Designate an (Assignment: organization-defined official) to manage the development, documentation, and dissemination of the incident response policy and procedures; and e. Review and update the current incident response; Policy (Assignment: organization-defined frequency); and f. Procedures (Assignment: organization-defined frequency).</td>
<td>This control addresses policy and procedures for the control in the B family that is implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate in their development. Security and privacy programs and policies and procedures at the organization level are preferable, in general, and may be dictated by the need for system-specific policies and procedures. This policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and policies that are system-specific, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in security and privacy plans or in one or more separate documents. Existing controls do not constitute an organizational policy or procedure.</td>
</tr>
<tr>
<td>IR-2</td>
<td>1</td>
<td>Incident Response</td>
<td>Incident Response Training</td>
<td>a. Provide incident response training to system users consistent with assigned roles and responsibilities; b. Within (Assignment: organization-defined time period) of assuming an incident response role or responsibility or acquiring system access; and c. When required by system changes; and d. (Assignment: organization-defined frequency) thereafter.</td>
<td>Incident response training is associated with assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and finally, incident responders may receive more specific training on forensic, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-2 or AT-3.</td>
</tr>
<tr>
<td>IR-8, PM-14</td>
<td>1</td>
<td>Incident Response</td>
<td>Incident Response Training</td>
<td>Incorporate simulated events into incident response training to facilitate the required response to potential crisis situations.</td>
<td>Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations.</td>
</tr>
<tr>
<td>IR-1</td>
<td>1</td>
<td>Incident Response</td>
<td>Incident Response Testing</td>
<td>Test the effectiveness of the incident response capability for the system (Assignment: organization-defined frequency) using the following tests: (Assignment: organization-defined tests);</td>
<td>Organizations test incident response capabilities to determine the effectiveness of the capability and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-throughs, tabletop exercises, and simulations.(parallel or full-interrupt). Incident response testing can include a determination of the effects on organizational operations, organizational assets, and individuals due to incident response. Use of qualitative and quantitative data sets in determining the effectiveness of incident response processes.</td>
</tr>
<tr>
<td>IR-10</td>
<td>1</td>
<td>Incident Response</td>
<td>Incident Response Testing</td>
<td>Test the incident response capability using (Assignment: organization-defined automated mechanisms);</td>
<td>Organizations use automated mechanisms to more thoroughly and affectively test incident response capabilities that can be accomplished by providing more complete coverage of incident response issues, by selecting more realistic test scenarios and test environments, and by stressing the response capability.</td>
</tr>
</tbody>
</table>
a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.
b. Coordinate incident handling activities with contingency planning activities.
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.
d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Organizations recognize that incident response capability is dependent on the capabilities of the organizational systems and the mission/business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources officers, physical security officers, pencil security offices, legal department, risk executive (function), operations personnel, procurement offices). Suspended security incidents include the receipt of suspicious e-mail communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. Suspended privacy incidents include a breach of personally identifiable information or the recognition that the processing of personally identifiable information causes potential privacy risk.

a. Support the incident handling process using (assignment: organization-defined automated mechanisms).
b. Automated mechanisms supporting incident handling processes include online incident management systems; and tools that support the collection of live response data, full-content packet capture, and forensic and recovery analysis.

Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for routers or firewalls. Organizations perform dynamic reconfiguration of systems, for example, to stop attackers, to incident satellites, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for enabling the reconfiguration of systems in the definition of the dynamic reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.

a. Implement a configurable capability to automatically disable the system if (assignment: organization-defined dynamic reconfiguration).
b. Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for routers or firewalls. Organizations perform dynamic reconfiguration of systems, for example, to stop attackers, to incident satellites, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for enabling the reconfiguration of systems in the definition of the dynamic reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.

a. Identify (assignment: organization-defined classes of incidents) and take the following actions in response to these incidents to ensure continuation of organizational missions and business functions (assignment: organization-defined actions to take in response to classes of incident).
b. Classes of incidents include malfunctions due to design or implementation errors and emissions, improper malicious attacks, and untargeted malicious attacks. Incident response actions include orderly system shutdown; system shutdown, fail to rescue mode or activation of alternative technology whereby the system operates differently, emulating alternative measures, alternate information flows, or operating in a mode that is reserved for when systems are under attack. Organizations consider whether continuity of operations requirements during an incident conflict with the capability to automatically disable the system as specified in paragraph 4-10(c).

a. Implement an incident handling capability for incidents involving insider threats.
b. While many organizations address insider threats as part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and the need for specific incident handling capability (as defined within organizations) to provide appropriate and timely responses.

a. Coordinate incident handling capability for insider threats that includes the following organizational entities (assignment: organization-defined entities). Incident handling for insider threats (including investigation, detection and analysis, containment, eradication, and recovery) requires coordination among many organizational entities, including mission or business owners, system owners, human resources officers, procurement offices, personnel offices, physical security officers, senior agency information security officer, operations personnel, risk executive (function), senior agency official for privacy, and legal counsel. In addition, organizations may require external support from federal state, and local law enforcement agencies.

a. Implement an incident handling capability (assignment: organization-defined dynamic response capability) to respond to incidents.
b. Dynamic response capability addresses the timely deployment of new or replacement organizational capabilities in response to incidents. This includes capabilities implemented at the mission and business process level and at the system level.

a. Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

Organizations involved in supply chain activities include product developers, system integrators, manufacturers, publishers, assemblers, distributors, vendors, and others. Supply chain incidents include compromises or breaches that impact system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations consider including processes for protecting and sharing incident information or information exchange agreements.
The incident response capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such capability.

### vulnerability related to incidents

Analysis of malicious code and other residual artifacts of a security or privacy incident can be helpful to the organization in improving techniques, tools, and procedures. It can also indicate the identity or some defining characteristics of the adversary. Malicious code analysis can also help the organization develop responses to future incidents.

### V-6 1 Incident Response | Incident Reporting

The incident reporting capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such capability.

### V-5 1 Incident Response | Incident Monitoring

Tracking and documenting security, privacy, and supply chain incidents.

Documenting incidents including maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensic and evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaint, supply chain partner, audit monitoring, physical access monitoring, and user and administrator reports.

### V-3 1 Incident Response | Incident Reporting | Automated Tracking, Data Collection, and Analysis

Automated mechanisms for tracking incidents and for collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

### V-2 1 Incident Response | Incident Reporting

The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

### V-1 1 Incident Response | Incident Reporting | Submission and Acceptance

To manage public requests associated with an incident, and b) Ensure that emergency and other pertinent information necessary for the organization is in a secure or structured environment.

The report should be submitted to the designated reporting authority or authorities.

### V-4 1 Incident Response | Incident Reporting | Automated Incident Response (including monitoring, scanning, and forensic tools to monitor, fuse, correlate, analyze, and respond to threats and security relevant events from multiple sources. These reports include perimeter defenses, network devices (e.g., routers, switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such capability.

### V-4 1 Incident Response | Incident Reporting | Security Operations Center

A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to identify and monitor an organization's systems and networks (e.g., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The organization staffs the SOC with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers) and implements a combination of technical, management, and operational control including monitoring, scanning, and forensic tools to monitor, fuse, correlate, analyze, and respond to threats and security relevant events from multiple sources. These reports include perimeter defenses, network devices (e.g., routers, switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such capability.

### V-4 1 Incident Response | Incident Reporting | Automated Incident Response

The reporting requirements are as specified in 18 C.F.R. Automated reporting mechanisms include email, posting on web sites, and automated incident response tools and programs.

### V-4 1 Incident Response | Incident Reporting | Vulnerabilities Related to Incidents

Report system vulnerabilities associated with reported incidents to the designated reporting authorities.

Reported incidents that uncover system vulnerabilities are analyzed by organizational personnel including system owners, mission/business owners, senior agency information security officers, senior agency officials for privacy, authorizing officials, and the risk executive (functions). The analysis can serve to prioritize and relate mitigation actions to address the discovered system vulnerability.

### V-4 1 Incident Response | Incident Reporting | Supply Chain Coordination

Provide security and privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.

Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packaging, assembly, distributors, vendors, and resellers. Supply chain incidents include compromises or breaches that result in the theft, modification, or destruction of hardware, software, data, intellectual property, or other information.

Incident response support resources provided by organizations include help desks, assistance groups, automated notification systems to open and track incident response tickets, and access to forensics services or consumer services websites, when required.

### V-1 1 Incident Response | Incident Response Assistance

Provide incident response support resources, integrates the organizational incident response capability, that offers advice and assistance to users of the system for handling and reporting of security, privacy, and supply chain incidents.
Initiate the availability of incident response information and support using (assignment: organization-defined automated mechanisms).

- Determine mechanisms to provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of improving understanding of current response capabilities and support.

- Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and
- Identify organizational response team members to external providers.

- External providers of system protection capability include the Computer Network Defense Program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks. It may be beneficial to have agreements in place with external providers to clarify the roles and responsibilities of each party before an incident occurs.

- SD-8

- 1 Incident Response | Incident Response Plan

- a. Develop an incident response plan that:
- b. Designate an (assignment: organization-defined official) to manage the development, documentation, and
- c. Alerting (assignment: organization-defined personnel or roles) of the incident information spill using a method of
- d. Isolating the contaminated system or component;
- e. Eradicating the information from the contaminated system or component;
- f. Identifying other systems or system components that may have been subsequently contaminated; and
- g. Protecting the incident response plan from unauthorized disclosure and modification.

- It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions and business functions help determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with other organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information, include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

- 2 Incident Response | Incident Response Plan | Privacy Breaches

- a. Include the following in the Incident Response Plan for breaches involving personally identifiable information:
- b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
- c. Identification of applicable privacy requirements.

- Organizations may be required by law, regulation, or policy to follow specific procedures relating to privacy breaches, including notice to individuals, affected organizations, and oversight bodies, standards of harm, and mitigation or other specific requirements.

- 3 Incident Response | Information Spillage Response

- a. Respond to information spills by:
- b. Information-spillage refers to instances where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of higher classification or impact level. At that point, corrective action is required. The nature of the response is based upon the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of contained storage media, and the access authorizations of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such isolation is isolated and evaluated.

- 4 Incident Response | Information Spillage Response | Recognition Processes

- a. Establish requirements for responding to information spillage incidents in incident response plans; incident response training on a regular basis helps to ensure that organizational personnel understand their individual responsibilities and what specific actions to take when spillage incidents occur.

- 5 Incident Response | Information Spillage Response | Post-spill Operations

- a. Corrective actions for systems contaminated due to information spills may be time-consuming. Personnel may not have access to the contaminated systems while corrective actions are being taken, which may potentially affect their ability to conduct organizational business.

- 6 Incident Response | Information Spillage Response | Exposure to Unauthorized Personnel

- a. Controls include ensuring that personnel who are exposed to spilled information are made aware of the laws, executive orders, directives, regulations, policies, standards, and guidelines regarding the information and the restrictions imposed based on exposure to such information.

- 7 Incident Response | Incident Analysis

- a. This control addresses policy and procedures for the MA family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are generally, and may obfuscate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the subject of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. NIST controls do not constitute an organizational policy or procedure.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA-2</td>
<td>1</td>
<td>Maintenance</td>
<td>Controlled Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Schedule, document, and review records of maintenance, repair, or replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Approve and monitor all maintenance activities, whether performed on-site or remotely, and whether the system or system components are serviced on-site or removed to another location;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Require that (Assignment: organization-defined personnel or roles) explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>d. Sanitize equipment to remove the following information from associated mediators prior to removal from organizational facilities for off-site maintenance, repair, or replacement: (Assignment: organization-defined information);</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement activities; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>f. Include the following information in organizational maintenance records: (Assignment: organization-defined information).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Controling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, printers, and printers. Information security for creating effective maintenance records includes date and time of maintenance; name of individuals or groups performing the maintenance; name of entity, if necessary, a description of the maintenance performed, and system components or equipment removed or replaced. Organizations consider supply chain issues associated with replacement components for systems.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-2 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Maintenance Tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve, control, and monitor the use of system maintenance tools; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review previously approved system maintenance tools (Assignment: organization-defined frequency).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-3 (2)</td>
<td>3</td>
<td>Maintenance</td>
<td>Automated Review</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Schedule, conduct, and document maintenance, repair, and replacement activities for the system using (Assignment: organization-defined automated mechanisms); and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Produce up-to-date, accurate, and complete records of maintenance, repair, and replacement activities requested, scheduled, or performed, and completed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-3 (1)</td>
<td>2</td>
<td>Maintenance</td>
<td>Maintenance Tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve, control, and monitor the use of system maintenance tools; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review previously approved system maintenance tools (Assignment: organization-defined frequency).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-3 (1)</td>
<td>2</td>
<td>Maintenance</td>
<td>Maintenance Tools</td>
<td>Inspection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-3 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Maintenance Tools</td>
<td>Inspection-Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Inspect media containing diagnostic and test programs for malicious code before the media are used in the system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Check media for unauthorized access to organizational information; and after the service is performed, inspect and sanitize the component (for organizational information); and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Require that (Assignment: organization-defined personnel or roles) explicitly approve the removal of the equipment from the facility.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-3 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Maintenance Tools</td>
<td>Unprotected Removal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Prevent the removal of system maintenance equipment containing organizational information by:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Verifying that there is no organizational information contained on the equipment;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Functioning or storing the equipment;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>d. Retaining the equipment within the facility; or</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>e. Obtaining an exemption from (Assignment: organization-defined personnel or roles) explicitly authorizing removal of the equipment from the facility.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-3 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Maintenance Tools</td>
<td>Prevent Unauthorized Removal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Log [Assignment: organization-defined audit events] for nonlocal maintenance and diagnostic sessions; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review the audit records of the maintenance and diagnostic sessions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-3 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Maintenance Tools</td>
<td>Prevent Unauthorized Removal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Log [Assignment: organization-defined audit events] for nonlocal maintenance and diagnostic sessions; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review the audit records of the maintenance and diagnostic sessions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-3 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Maintenance Tools</td>
<td>Automated Review</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Schedule, conduct, and document maintenance, repair, and replacement activities for the system using (Assignment: organization-defined automated mechanisms); and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Produce up-to-date, accurate, and complete records of maintenance, repair, and replacement activities requested, scheduled, or completed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve and monitor noncritical maintenance and diagnostic activities only as consistent with organizational policy and documented in the security plan for the system;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Monitor security-related issues associated with maintenance tools that are not within the system's boundaries but that are used specifically for diagnostic and repair activities.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Software Update and Patch</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Inspect maintenance tools to ensure the latest software updates and patches are installed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Maintenance tools using outdated and/or unsupported software can provide a threat vector for adversarial and result in significant vulnerability for organizations.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>3</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Software Update and Patch</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve and monitor noncritical maintenance and diagnostic activities only as consistent with organizational policy and documented in the security plan for the system;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Include the following information in organizational maintenance records:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>i. Name of escort, if necessary; ii. A description of the maintenance performed; iii. Name of entity, if necessary; iv. A description of the maintenance performed, and system components or equipment removed or replaced.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Authorization and Assurnment of Maintenance Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Ensure that noncritical maintenance and diagnostic services are performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Remove the component to be serviced from the system prior to noncritical maintenance or diagnostic services and the component (or organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reinserting the component to the system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Authorization and Assurnment of Maintenance Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Inspect noncritical maintenance services by:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Comparing security capability on systems, diagnostic tools, and equipment providing maintenance services to the mechanisms that implement controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Authorization and Assurnment of Maintenance Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Inspect noncritical maintenance services by:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Comparing security capability on systems, diagnostic tools, and equipment providing maintenance services to the mechanisms that implement controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Authorization and Assurnment of Maintenance Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Inspect noncritical maintenance services by:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Inspect the audit records of maintenance and diagnostic sessions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Authorization and Assurnment of Maintenance Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Inspect the audit records of maintenance and diagnostic sessions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Approval and Authorizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve and control the use of system maintenance tools; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review previously approved system maintenance tools (Assignment: organization-defined frequency).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Approval and Authorizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve and control the use of system maintenance tools; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review previously approved system maintenance tools (Assignment: organization-defined frequency).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Approval and Authorizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve and control the use of system maintenance tools; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review previously approved system maintenance tools (Assignment: organization-defined frequency).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Approval and Authorizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve and control the use of system maintenance tools; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review previously approved system maintenance tools (Assignment: organization-defined frequency).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MA-4 (2)</td>
<td>2</td>
<td>Maintenance</td>
<td>Noncritical Maintenance</td>
<td>Approval and Authorizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Approve and control the use of system maintenance tools; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Review previously approved system maintenance tools (Assignment: organization-defined frequency).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MA-4 (1) 2 Maintenance | Nonlocal Maintenance | Cryptographic Protection  
implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: (Assignment: organization-defined cryptographic mechanisms).  

- To protect nonlocal maintenance and diagnostic communications, mechanisms must be implemented.  
- Mechanisms may be a combination of hardware, software, and procedural controls.  
- Mechanisms must be documented in security plans for the systems.

MA-4 (7) 2 Maintenance | Nonlocal Maintenance | Disconnected Verification  
Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.  

- This control enhancement ensures that connections established during nonlocal maintenance and diagnostic sessions have been terminated and are no longer available for use.

MA-5 1 Maintenance | Maintenance Personnel  
(a) Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;  
(b) Invo-duce automated mechanisms.  

- This control enhancement ensures that maintenance personnel are authorized.  
- Automated mechanisms are used to ensure compliance with the control requirement.

MA-5 (1) 2 Maintenance | Maintenance Personnel | Individuals Without Appropriate Access  
(c) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:  
(d) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances, or formal access approvals, all sensitive information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
(e) Develop and implement (Assignment: organization-defined alternate controls) in the event a system component cannot be sanitized, removed, or disconnected from the system.

- Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are used to ensure that maintenance personnel are appropriately authorized.

MA-5 (2) 2 Maintenance | Maintenance Personnel | Security Clearance for Classified Systems  
Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.

- Personnel conducting maintenance on systems may be exposed to classified information during the course of their maintenance activities.  
- Procedures for the use of maintenance personnel can be documented in security plans for the systems.

MA-5 (3) 2 Maintenance | Maintenance Personnel | Citizenship Requirements for Classified Systems  
Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.

- Personnel conducting maintenance on systems may be exposed to classified information during the course of their maintenance activities.  
- Procedures for the use of maintenance personnel can be documented in security plans for the systems.

MA-5 (1) 2 Maintenance | Maintenance Personnel | Foreign Nationals  
Verify that:  
(a) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and
(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are formalized within Memos of Understandings.

- Personnel conducting maintenance on systems may be exposed to classified information during the course of their maintenance activities.  
- Procedures for the use of maintenance personnel can be documented in security plans for the systems.

MA-5 (2) 2 Maintenance | Maintenance Personnel | Non-system Maintenance  
Verify that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

- Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the function provided by those components is not operational.  
- Organizations retain maintenance support include having appropriate contracts in place.

MA-6 1 Maintenance | Timely Maintenance  
Observe maintenance support and/or spare parts for (Assignment: organization-defined system components) within (Assignment: organization-defined time period) of failure.

- Preventive maintenance activities in other capacities not directly related to the system include physical plant personnel and custodial personnel.

MA-6 (1) 2 Maintenance | Timely Maintenance | Preventive Maintenance  
Perform preventive maintenance on (Assignment: organization-defined system components) at (Assignment: organization-defined time interval).

- Preventive maintenance includes proactive care and the servicing of system components to maintain organizational equipment and facilities in satisfactory operating condition.  
- Such preventive maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects.  
- The primary goal of preventive maintenance is to avoid or mitigate the consequences of equipment failures.  
- Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they fail.  
- Methods of determining when preventive or other failure management actions should be applied include original equipment manufacturer recommendations, statistical failure records, expert opinion, maintenance that has already been conducted on similar equipment, requirements of codes, laws, or regulations within a jurisdiction; or measured values and performance indicators.

MA-6 (2) 2 Maintenance | Timely Maintenance | Predictive Maintenance  
Perform predictive maintenance on (Assignment: organization-defined system components) at (Assignment: organization-defined time interval).

- Predictive maintenance evaluates the condition of equipment by performing periodic or continuous (safely equipment condition monitoring).  
- The goal of predictive maintenance is to perform maintenance at a scheduled time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold.  
- The predictive component of predictive maintenance stems from the objective of predicting the future trend of the equipment’s condition.  
- The predictive maintenance approach employs principles of statistical process control to determine at what point in the future maintenance activities will be appropriate.  
- Most predictive maintenance inspections are performed while equipment is in service, thus, minimizing disruption of normal system operations.  
- Predictive maintenance can result in substantial cost savings and higher system reliability.

MA-6 (1) 2 Maintenance | Timely Maintenance | Automated Support for Predictive Maintenance  
Transfer predictive maintenance data to a maintenance management system using (Assignment: organization-defined automated mechanisms).

- A computerized maintenance management system contains a database of information about the maintenance operations of organizations and automates processing equipment condition data to trigger maintenance planning, execution, and reporting.
### MP-2 1 Media Access Controls

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restrict access to</strong></td>
<td>Assignment: organization-defined types of digital and/or non-digital media to Assignment: organization-defined personnel or roles.</td>
</tr>
<tr>
<td><strong>Protect system media</strong></td>
<td>Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (solid state, magnetic), compact disks, and digital video discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individual seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact disk in the media library is an example of restricting access to digital media.</td>
</tr>
</tbody>
</table>

### MP-3 1 Media Protection

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect and control</strong></td>
<td>Assignment: organization-defined types of system media during transport outside of controlled areas using Assignment: organization-defined controls.</td>
</tr>
<tr>
<td><strong>Maintain accountability for</strong></td>
<td>System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (solid state, magnetic), compact disks, and digital video discs. Non-digital media includes paper and microfilm. Security marking refers to the application or use of human-readable security attributes. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require marking for public information indicating that the information is publicly releasable. System media marking affects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.</td>
</tr>
</tbody>
</table>

### MP-4 1 Media Storage

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physically control and securely store</strong></td>
<td>Assignment: organization-defined types of digital and/or non-digital media within Assignment: organization-defined controlled areas; and</td>
</tr>
<tr>
<td><strong>Protect system media</strong></td>
<td>System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (solid state, magnetic), compact disks, and digital video discs. Non-digital media includes paper and microfilm. Physical controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet; or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. For media containing information determined to be in the public domain, to be publicly releasable, or to have limited adverse impact on organizations, operations, or individuals if accessed by other than authorized personnel, fewer controls may be needed. In these situations, physical access control provide adequate protection.</td>
</tr>
</tbody>
</table>

### MP-5 1 Media Transport

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect and control</strong></td>
<td>Assignment: organization-defined types of system media during transport outside of controlled areas using Assignment: organization-defined controls.</td>
</tr>
<tr>
<td><strong>Maintain accountability for</strong></td>
<td>System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (solid state and magnetic), compact disks, and digital video discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport process, and the actual transport. Transported and/or carrier personnel may include individuals external to the organization. Maintaining accountability for media during transport includes restricting transport activities to authorized personnel, and tracking and/or storing records of transport activities as the media moves through the transport process.</td>
</tr>
<tr>
<td>Control ID</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>MP-6 (1)</td>
<td>Display an identified custodian during transport of system media outside of controlled areas.</td>
</tr>
<tr>
<td>MP-6 (2)</td>
<td>Media Protection</td>
</tr>
<tr>
<td>MP-6 (3)</td>
<td>Purge or wipe information from assignments: organization-defined systems or systems components</td>
</tr>
<tr>
<td>MP-6 (4)</td>
<td>Remote Purge or Wipe Information</td>
</tr>
</tbody>
</table>

Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media such as scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media such as paper and microfilm. The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erasure, de-identification of personally identifiable information, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization method 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 information deemed to have no adverse impact on an organization or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. Mobile policies control the sanitization process for controlled unclassified information. NSA standards and policies control the sanitization process for media containing classified information.

Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media such as scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media such as paper and microfilm. The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erasure, de-identification of personally identifiable information, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization method 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 information deemed to have no adverse impact on an organization or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. Mobile policies control the sanitization process for controlled unclassified information. NSA standards and policies control the sanitization process for media containing classified information.
a. Establish [Assignment: organization-defined system media downgrading process] that includes employing [Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on the system. 

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and associated physical and environmental protection controls; 

c. Restate and update the current physical and environmental protection policy that: (a) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and (b) is consistent with applicable controls to restrict the use of system media. Organizations can document the media downgrading processes by providing information such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

d. Remove individuals from the facility access list when access is no longer required.

e. Document system media downgrading actions. Organizations can document the media downgrading process by providing information such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

2. Procedures [Assignment: organization-defined frequency].

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 

1. [Selection (one or more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that: 

a. Determine [Assignment: organization-defined personnel or roles]: 

1. [Selection (one or more): system media; media requiring downgrading]; and 

2. Selection (one or more): physical access authorizations; access by position or role.

2. [Assignment: organization-defined list of acceptable forms of identification].

3. A list of individuals with authorized access to the facility where the system resides; 

4. A list of individuals with authorized access to the system media; 

5. A list of individuals with authorized access to the facility where the system resides.

b. Test downgrading equipment and procedures [Assignment: organization-defined frequency] to verify that downgrading actions are being achieved.

c. Document system media downgrading actions.

d. Downgrade system media containing classified unclassified information prior to public release.

3. Procedures [Assignment: organization-defined frequency].

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 

1. [Selection (one or more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that: 

a. Allocate and assign responsibilities for the security and privacy programs and for access to media, MP-7 restricts the use of certain types of media on systems, for example, prohibiting the use of flash drives or external hard disk drives. Organizations use technical and non-technical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical means to prevent access to certain external ports, or disabling or 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 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 writable, portable storage devices, and implementing this restriction by disabling or removing the ability to write to such devices requiring identifiable owners for storage devices reduce the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

b. Recognize physical access to the facility where the system resides. 

2. Procedures [Assignment: organization-defined frequency].

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; 

b. Issue authorization credentials for facility access; 

c. Review the list of detailed authorized facility access by individuals [Assignment: organization-defined frequency]; and 

d. Remove individuals from the facility access list when access is no longer required.

3. Procedures [Assignment: organization-defined frequency].

a. Identify [Assignment: organization-defined system media requiring downgrading]; and 

b. Identify [Assignment: organization-defined list of acceptable forms of identification].

This control addresses policy and procedures for the controls in the PS-5 family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for systems specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Operating controls do not constitute an organizational policy or procedure.

b. Authorize physical access to the facility where the system resides based on position or role.

3. Procedures [Assignment: organization-defined frequency].

a. Require two forms of identification from the following forms of identification for visitor access to the facility: 

b. Authorize physical access to the facility where the system resides based on position or role. Role-based facility access includes permanent maintenance personnel, duty officers, or emergency medical staff.
Control ID | Level | Control Name | Withdrawn | Control Text | Discussion | Related Controls | Notes
---|---|---|---|---|---|---|---
PE-3 | 2 | Physical and Environmental Protection | Monitoring | PE-3 (2) Physical and Environmental Protection | Physical | PE-8, PE-7, PE-2, PE-3, RA-3, SC-5, PE-9, AU-13, CP-10, IA-3, AT-3, AU-2, AU-6, AU-11, DF-10, WR-6, MS-5, MP-2, MP-4, PA-5, PA-C, PE-4, PC-14, PC-9, PE-8, PE-5, PE-7, PE-11, SC-18, SI-1, SI-3

**Control Text:**

1. **Physical and Environmental Protection | Physical Access Control**
   - a. Enforce physical access authorizations at [assignment: organization-defined entry and exit points to the facility where the system resides] by:
     1. Verifying individual access authorizations before granting access to the facility, and
     2. Controlling signs and access to the facility using detection (i.e., rain or menu; Assignment: organization-defined physical access control systems or devices; guards).
   - b. Maintain physical access audit logs for [assignment: organization-defined entry or exit points];
   - c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [assignment: organization-defined controls];
   - d. Escort visitors and monitor visitor activity [assignment: organization-defined circumstances requiring visitor access and monitoring];
   - e. Secure keys, combinations, and other physical access devices;
   - f. Inventory [assignment: organization-defined devices, keys; Assignment: organization-defined frequency]; and
   - g. Change combinations and keys [assignment: organization-defined frequency] and/or when keys are lost; combinations are compromised; or when individuals possessing the keys or combinations are transferred or terminated.

2. **Physical and Environmental Protection | Physical Access Control | Physical Security**
   - a. Deploy guests to control [assignment: organization-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.

3. **Physical and Environmental Protection | Physical Access Control | Access Control | Control Name**
   - a. Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [assignment: organization-defined physical spaces containing one or more components of the system].
   - b. Maintain physical access audit logs for [assignment: organization-defined entry or exit points] to the facility or system for反映了information or removal of system components.
   - c. Control access to areas within the facility deemed as publicly accessible or protected areas.
   - d. Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [assignment: organization-defined locations within the facility].

4. **Physical and Environmental Protection | Physical Access Control | Monitored Access**
   - a. Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [assignment: organization-defined entry and exit points to the facility or system for reflected information or removal of system components].

5. **Physical and Environmental Protection | Physical Access Control | Out of Band Access**
   - a. Ensure physical access to the facility where the system resides and responds to physical security incidents;
   - b. Review physical access logs [assignment: organization-defined frequency] and upon occurrence of [assignment: organization-defined events or potential indications of events]; and
   - c. Coordinate results of reviews and investigations with the organizational incident response capability.

6. **Physical and Environmental Protection | Physical Access Control | Access Control | Facility and Systems**
   - a. Implement access control vestibules at [assignment: organization-defined locations within the facility]. An access control vestibule, or mantrap, is part of a physical access control system that typically provides a space between two sets of interlocking doors. Access control vestibules are designed to prevent unauthorized individuals from following authorized individuals into facilities with controlled access. This activity, also known as piggybacking or tailgating, results in unauthorized access to the facility. Access control vestibules can also be used to limit the number of individuals entering controlled access points and to provide containment areas to verify credentials. Access control vestibules can be fully automated, controlling the opening and closing of the interlocking doors; or partially automated using security guards to control the number of individuals entering the facilities.

**Related Controls:**

- AU-2, AU-6, AU-13, DF-10, WR-6, MS-5, MP-2, MP-4, PA-5, PA-C, PE-4, PC-14, PC-9, PE-8, PE-5, PE-7, PE-11, SC-18, SI-1, SI-3

**Notes:**

- [Assignment: organization-defined events or potential indications of events]; and
- [Assignment: organization-defined system output devices];
- [Assignment: organization-defined output devices];
- [Assignment: organization-defined frequency]; and
- [Assignment: organization-defined controls].
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE-8 (1)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.</td>
<td>PE-12 1 Physical and Environmental Protection</td>
<td>Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-8 (2)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>Recognize (Assignment: organization-defined classes or types of intrusions) and initiate (Assignment: organization-defined response actions) using (Assignment: organization-defined automated mechanisms).</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>Recognize (Assignment: organization-defined classes or types of intrusions) and initiate (Assignment: organization-defined response actions) using (Assignment: organization-defined automated mechanisms).</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-8 (3)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-6 (4) 2 Physical and Environmental Protection</td>
<td>PE-6 (3) 2 Physical and Environmental Protection</td>
<td>PE-6 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-8 (4)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-15 1 Physical and Environmental Protection</td>
<td>PE-4 1 Physical and Environmental Protection</td>
<td>PE-9 1 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-8 (5)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-8 1 Physical and Environmental Protection</td>
<td>PE-9 1 Physical and Environmental Protection</td>
<td>PE-10 1 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-8 (6)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-8 (7)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-11 (2) 2 Physical and Environmental Protection</td>
<td>PE-9 1 Physical and Environmental Protection</td>
<td>PE-10 1 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-9 (1)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-9 (2)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-10 (1)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-10 (2)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-10 (3)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-11 (1)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-11 (2)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-11 (3)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
<tr>
<td>PE-12 (1)</td>
<td>2</td>
<td>Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-11 (1) 2 Physical and Environmental Protection</td>
<td>PE-12 (1) 2 Physical and Environmental Protection</td>
<td>PE-10, PE-11, PE-12</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- PE-10: Withdrawn (Incorporated into PE-12, PE-13).
- PE-11: Withdrawn (Incorporated into PE-12).

**Discussion:**
- Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems are used in conjunction with physical barriers, physical access control systems, and security guards, triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, for example, motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

**Control Text:**
- PE-12: Recognize (Assignment: organization-defined classes or types of intrusions) and initiate (Assignment: organization-defined response actions) using (Assignment: organization-defined automated mechanisms).
- PE-11: Recognize (Assignment: organization-defined classes or types of intrusions) and initiate (Assignment: organization-defined response actions) using (Assignment: organization-defined automated mechanisms).
- PE-10: Recognize (Assignment: organization-defined classes or types of intrusions) and initiate (Assignment: organization-defined response actions) using (Assignment: organization-defined automated mechanisms).

**Related Controls:**
- PE-12: PE-11, PE-10, PE-12
- PE-11: PE-10, PE-11, PE-12
- PE-10: PE-12, PE-11, PE-10

**Notes:**
- PE-10 is withdrawn (Incorporated into PE-12, PE-13).
- PE-11 is withdrawn (Incorporated into PE-12).

**Related Controls:**
- PE-6: PE-10, PE-11, PE-12
- PE-8: PE-10, PE-11, PE-12
- PE-9: PE-10, PE-11, PE-12
- PE-10: PE-12, PE-11, PE-10
- PE-11: PE-10, PE-11, PE-12
- PE-12: PE-10, PE-11, PE-12

**Notes:**
- PE-10 is withdrawn (Incorporated into PE-12, PE-13).
- PE-11 is withdrawn (Incorporated into PE-12).
- PE-12 is withdrawn (Incorporated into PE-12, PE-13).
**PE-18** 1 Physical and Environmental Protection | Fire Protection

Deploy and maintain fire detection and suppression systems that are supported by an independent energy source.

The provisions of fire detection and suppression systems apply to organizational facilities containing concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems, fixed foam, and smoke detectors.

**PE-19** 1 Physical and Environmental Protection | Information Leakage

Protect the system from information leakage due to electromagnetic signals emanations.

Information leakage is the intentional or unintentional release of data or information to an unauthorized environment from electromagnetic signals emanations. The security categories or classifications of systems (with respect to confidentiality), organizational security policies, and risk tolerance guide the selection of controls employed to protect systems against information leakage due to electromagnetic signals emanations.

**PE-21** 1 Physical and Environmental Protection | Electromagnetic Pulse Protection

Employ [assignment: organization-defined controls] against electromagnetic pulse damage for [assignment: organization-defined systems and system components].

An electromagnetic pulse (EMP) is a short burst of electromagnetic energy that is spread over a range of frequencies. Such energy bursts may be natural or man-made. EMP-interference may be disruptive or damaging to electronic equipment. Protective measures used to mitigate EMP risk include shielding, surge suppressors, fire-resistant transformers, and earth grounding.

**Notes**

Withdrawn: Incorporated into PE-12(2).

Withdrawn: Incorporated into PE-12(2).
PL-23 1 Physical Environmental Protection | Facility Planning

a. Plan the location or site of the facility where the system resides considering physical and environmental hazards.

b. For existing facilities, consider the physical and environmental hazards in the organization's risk management strategy.

PL-22 1 Physical Environmental Protection | Facility Planning

Mark [assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.

PL-1 2 Planning | Policy and Procedures

a. Develop security and privacy plans for the system that:

0. Develop and distribute to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-defined personnel or roles];

2. [Withdrawn: Incorporated into PL-2];

3. [Assignment: organization-defined personnel or roles]

X. Address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

b. Are consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;

c. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

d. Design or [Assignment: organization-defined personnel or roles] to manage, develop, disseminate, and review the planning policy and procedures;

e. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

f. Protect the plans from unauthorized disclosure and modification.

Security plans may be developed for both existing and new systems. Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that address security and privacy requirements contained in or referenced by that system's security and privacy policy or can be represented by multiple policies reflecting the complex nature of the system. Procedures can be established for security and privacy programs and for implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, and the Nation if the plans are implemented. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be communicated in written and oral form and can be documented in system security and privacy plans or in one or more separate documents. Limiting controls do not constitute an organizational policy or procedure.

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing information to access to the system and any dependencies on or connections to other systems or system components;

e. Identify any relevant control baselines or overviews, if applicable;

f. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

2. [Assignment: organization-defined individual or groups]; and

3. [Assignment: organization-defined individual or groups]; and

b. Receive a documented acknowledgment 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 system;

c. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-

PL-1 1 Planning | Policy and Procedures

a. Develop security and privacy plans for the system that:

X. [Assignment: organization-defined personnel or roles];

b. Are consistent with the organization's enterprise architecture;

c. Security and privacy plans need not contain detailed contingency plan development life cycle, systems engineering, and acquisition. Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that address security and privacy requirements contained in or referenced by that system's security and privacy policy or can be represented by multiple policies reflecting the complex nature of the system. Procedures can be established for security and privacy programs and for implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, and the Nation if the plans are implemented. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be communicated in written and oral form and can be documented in system security and privacy plans or in one or more separate documents. Limiting controls do not constitute an organizational policy or procedure.

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

b. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

c. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

PL-1 2 Planning | System Security and Privacy Plans

a. Develop security and privacy plans for the system that:

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

b. drafting, document, and distribute to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-defined personnel or roles];

2. [Assignment: organization-defined personnel or roles];

PL-1 1 Planning | System Security and Privacy Plans

a. Develop security and privacy plans for the system that:

X. Develop security and privacy plans for the system that:

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

b. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

c. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

PL-1 2 Planning | System Security and Privacy Plans

a. Develop security and privacy plans for the system that:

2. [Assignment: organization-defined personnel or roles];

3. [Assignment: organization-defined personnel or roles];

PL-1 1 Planning | System Security and Privacy Plans

a. Develop security and privacy plans for the system that:

X. Develop security and privacy plans for the system that:

6. Identify any relevant control baselines or overviews, if applicable;

c. Identify any relevant control baselines or overviews, if applicable;

d. Identify any relevant control baselines or overviews, if applicable;

b. Identify any relevant control baselines or overviews, if applicable;

c. Identify any relevant control baselines or overviews, if applicable;

e. Identify any relevant control baselines or overviews, if applicable;

b. Identify any relevant control baselines or overviews, if applicable;

e. Identify any relevant control baselines or overviews, if applicable;

d. Identify any relevant control baselines or overviews, if applicable;

b. Identify any relevant control baselines or overviews, if applicable;

c. Identify any relevant control baselines or overviews, if applicable;

d. Identify any relevant control baselines or overviews, if applicable;

e. Identify any relevant control baselines or overviews, if applicable;

b. Receive a documented acknowledgment 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 system;

c. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-

PL-1 2 Planning | System Security and Privacy Plans

a. Develop security and privacy plans for the system that:

X. Develop security and privacy plans for the system that:

b. Receive a documented acknowledgment 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 system;

c. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-

PL-8 1 Planning | Security and Privacy Architectures

a. Develop security and privacy architectures for the system that:
   i. Describe the requirements and approaches to be taken for protecting the confidentiality, integrity, and availability of organizational information;
   ii. Describe the requirements and approaches to be taken for processing personally identifiable information to minimize privacy risks to individuals;
   iii. Describe how the architectures are integrated into and support the enterprise architecture; and
   iv. Describe any assumptions about, and dependencies on, external systems and services; review, and update the architectures (Assignment: organization-defined frequency) to reflect changes in the enterprise architecture; and
   v. Reflect planned architecture changes in the security and privacy plans, the Concept of Operations (CONOPS), organizational procedures, and procurements and acquisitions.

b. Review and update the CONOPS (Assignment: organization-defined frequency).

c. Reflect planned architecture changes in the security and privacy plans, the Concept of Operations (CONOPS), organizational procedures, and procurements and acquisitions.

d. Ensure that the allocated controls operate in a coordinated and mutually reinforcing manner.

e. Ensure that the allocated controls work together to provide overall security and privacy protection.

f. Review and update the CONOPS (Assignment: organization-defined frequency).

The system-level security and privacy architectures are consistent with organizational wide security and privacy architectures described in PL-7. They are integral and developed as part of the enterprise architecture. The system-level security and privacy architectures are used to describe how the confidentiality, integrity, and availability of organizational information, security- and privacy-related information for external consumers, information being exchanged across organizational boundaries, and the protection mechanisms associated with each interface. The architectures can also include, for example, user roles and the access privileges assigned to each role; security and privacy operational procedures and policies; security-related information for external interfaces, information being exchanged across organizational boundaries, and the protection mechanisms associated with each interface. The architectures can also include, for example, user roles and the access privileges assigned to each role; security and privacy operational procedures and policies; security-related information for external interfaces, information being exchanged across organizational boundaries, and the protection mechanisms associated with each interface. The CONOPS is a living document that requires updating throughout the system development life cycle and is maintained by the security and privacy architecture and planning organization.

The CONOPS may be included in the security or privacy plans for the system or in other systems development life cycle documents. The CONOPS is a living document that requires updating throughout the system development life cycle. For example, during system design reviews, the concept of operations is checked to ensure that it remains consistent with the design for controls, the system architecture, and the operational procedures. Changes to the CONOPS are reflected in ongoing updates to the security and privacy architectures, and other appropriate organizational documents, for example, procurement specifications, systems development life cycle documents, and systems engineering documents.

Notes

AS-1, CM-6, CM-9, CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-7, SI-8.
Control baselines are pre-defined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to satisfy mandates imposed by law, executive orders, directives, regulations, policies, standards, or guidelines; or to address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of federal agencies' privacy, information, and information systems, with subsequent tailoring actions to manage risk in accordance with mission, business, or other considerations (see PL-11). Federal control baselines are provided in SP 800-53B. The selection of a control baseline is determined by the needs of stakeholders. Stakeholder needs consider mission and business requirements and as well as mandates imposed by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. For example, the control baselines in SP 800-53B are based on the requirements from [FISMA] and [PRIVACT]. The requirements, along with the NIST standards and guidelines implementing the legislation, direct organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system, analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations or the Nation; and considering the results from system and organizational risk assessments.

PL-21 1 Planning | Baseline Tailoring
Take the selected control baseline by applying specified tailoring actions.

PM 0 Program Management

PM-1 1 Program Management | Information Security
Program Plan
a. Develop and disseminate an organization-wide information security program plan that:
   i. 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; ii. Includes the identification and assignment of roles, responsibilities, management commitments, coordination among organizational entities, and compliance; iii. Reflects the coordination among organizational entities responsible for information security; and iv. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including missions, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
   b. Review the organization-wide information security program plan (Assignment: organization-defined frequency); c. Update the information security program plan to address organizational changes and problems identified during plan implementation or control assessments; and d. Protect the information security program plan from unauthorized disclosure and modification.

PM-2 1 Program Management | Information Security
Program Leadership Role
Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

PM-3 1 Program Management | Information Security and Privacy Resources
a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines; and c. Make available for expenditure, the planned information security and privacy resources.

PM-4 1 Program Management | War of Action and Millenarian Processes
a. Implement a process to ensure that plans of action and milestones for the information security and privacy programs and associated organizational systems are:
   i. Developed and maintained; ii. Document the remediation information security and privacy actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and iii. Are reported in accordance with established reporting requirements; b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-5 1 Program Management | System Inventory
Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.

Notes:
PL-11, RA-2, RA-4, SA-6, SA-8
PL-21, RA-2, RA-4, SA-6, SA-8
PM-1, FMA-10, PM-12, RA-11, SI-2.1
PM-2, SI-2.3
PM-3, SI-2.4
PM-4, CA-7, PM-4, RA-12, SI-5.6
PM-5, CA-6, CA-7, PM-4, SA-5
PM-6 1 Program/Management | Measures of Performance
Develop, monitor, and report on the results of information security and privacy measures of performance. Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the controls employed in support of the program.

PM-7 1 Program/Management | Enterprise Architecture
Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation. The architecture and its security and privacy requirements and controls into the enterprise architecture help to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly linked to the organization’s mission and business processes. The process of security and privacy requirements and controls integration also embodies into the enterprise architecture, the organization’s security and privacy architectures consistent with the organizational risk management strategy. For PM-7, security and privacy architectures are developed at a system of systems level, representing all organizational systems. For PM-8, the security and privacy architectures are developed at a level representing an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework (SP 800-37) and supporting security standards and guidelines.

PM-7 (1) 2 Program/Management | Enterprise Architecture
Offload (assignment: organization-defined non-essential functions or services) to other systems, system components, or an external provider. Not every function or service a system provides is essential to an organization’s mission or business operations. Printing or copying is an example of a non-essential but supporting service for an organization. Wherever feasible, such supportive but non-essential functions or services are not co-located with the functions or services supporting essential missions or business operations. Outsourcing such functions on the same system or system component increases the attack surface of the organization’s mission essential functions or services. Depending on how the support function and designated authorizing official for each system, system component, or external provider can also improve efficiency by putting those functions or services under the control of individuals or providers who are subject-matter experts in the functions or services.

PM-8 1 Program/Management | Critical Infrastructure Plan
Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. Protection strategies are based on the prioritization of critical assets and resources. The guidance and rationale for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

PM-9 1 Program/Management | Risk Management Strategy
Develop a comprehensive strategy to manage:
1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; and
3. Implement the risk management strategy consistently across the organization; and
4. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization; security and privacy risk mitigation strategies; acceptable risk assessment methodologies; a process for evaluating security and privacy risk; information security and privacy risk assessment tools; and across the organization with respect to the organization’s risk tolerance; and approaches for managing risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security and privacy management processes with strategies, operating, and budgetary-planning processes. The risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization wide. The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure the strategy is broad-based and comprehensive.

PM-10 1 Program/Management | Authorization Process
a. Manage the security and privacy state of organizational systems and the environments in which these systems operate through authorization processes.
1. Designate individuals to fill specific roles and responsibilities within the organizational risk management process; and
2. Integrate the authorization processes into an organization-wide risk management program.

Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive function and designated authorizing official for each organizational system and common control provider. The organizational authorization processes are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

PM-11 1 Program/Management | Mission and Business Process Definition
a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and
c. Review and revise the mission and business processes [Assignment: organization-defined frequency].

Protection needs are technology-independent, required capabilities to counter threats to information systems, including, but not limited to, confidentiality, integrity, availability, or privacy. Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by the stakeholders in organizations, the mission and business processes defined to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required controls for the organization and the systems, inherent in defining protection and personally identifiable information processing needs, is an understanding of adverse impact that could result if a compromise or breach of information occurs. The integration process is used to map such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of authorized processing of information at any stage of the data life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policy and procedures.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM-12</td>
<td>1</td>
<td>Program/Management</td>
<td>Program/Management</td>
<td>Implement an insider threat program that includes a cross-discipline insider threat incident handling team.</td>
<td>Organizations handling classified information are required, under Executive Order 13516 (EO 13516) and the National Insider Threat Policy (NITP), to establish insider threat programs. The same standards and guidelines that apply to insider threat programs in classified environments can be employed effectively to improve the security of controlled unclassified and other information in non-national security systems. Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integration and analysis of threat information and observables. Threat information (i.e., indicators and warnings about threats) is collected from various sources. The threat information collected includes, but is not limited to, information that is processed, stored or transmitted on external systems. Observables are indicators that sensors need to be searching for. By utilizing well known patterns of behavior and observable characteristics, organizations can more accurately identify malicious insider activity. Insider threat programs are required to develop and impose a policy for the program to address in the centralized integration and analysis capability. Insider threat programs require organizations to prepare department or agency insider threat policies and implementation plans; conduct threat-based vulnerability assessments and monitoring activities; conduct assessments of department or agency insider threat policies and implementation plans; conduct host-based user monitoring of individual employee activities on government-owned classified computer systems; provide insider threat awareness training in conjunction with access control training from offices in the department or agency for insider threat analysis; and conduct self-assessments of department or agency insider threat policies. Insider threat programs leverage the expertise of all incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as they are compelling evidence to show that some types of insider crime can often be preceded by nontechnical behaviors in the workplace, including ongoing patterns of disruptive behavior and conflicts with coworkers and other colleagues. Human resources records could also identify potential risks if more focused, targeted monitoring efforts. The use of human resource records could raise significant concerns for privacy. The participation of a single team, including consultation with the senior agency official for privacy, ensures that monitoring activities are performed in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.</td>
</tr>
<tr>
<td>CA-6, AT-1, AT-9, PS-3, PS-4, PS-5, PS-7, PS-8, SC-5, SC-6, SC-9-14, FM-14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PM-13</td>
<td>1</td>
<td>Program/Management</td>
<td>Security and Privacy Workforce</td>
<td>Establish a security and privacy workforce development and improvement program.</td>
<td>Security and privacy workforce development and improvement programs include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks, developing role-based training programs for individuals assigned security and privacy roles and responsibilities, and providing standards and guidelines for measuring and building individual qualifications for incumbent and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to frequently assess and track the security and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities needed to protect organizational operations, assets, and individuals.</td>
</tr>
<tr>
<td>AT-2, AT-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PM-14</td>
<td>1</td>
<td>Program/Management</td>
<td>Testing, Training, and Monitoring</td>
<td>a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems and processes are developed and maintained.</td>
<td>This control ensures that organizations provide oversight for testing, training, and monitoring activities and that those actions are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and conduct testing and monitoring activities that are not conducted as part of ongoing assessments supporting a variety of controls. Security and privacy training activities, while focused on individual systems and specific roles, require coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.</td>
</tr>
<tr>
<td>AT-1, AT-3, CA-1, CA-12, IA-4, IA-8, FM-12, SI-4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PM-15</td>
<td>1</td>
<td>Program/Management</td>
<td>Security and Privacy Groups and Associations</td>
<td>Establish and maintain contact with wider groups and associations within the security and privacy communities.</td>
<td>Establishing contact with security and privacy groups and associations is important in an environment of rapidly changing technologies and threats. Groups and associations include special interest groups, professional associations, forums, news groups, user groups, and peer groups of security and privacy professionals in similar organizations. Organizations leverage security and privacy groups and associations based on missions and business functions. Organizational share threat, vulnerability, and incident information as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.</td>
</tr>
<tr>
<td>AA-1, IA-5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PM-16</td>
<td>1</td>
<td>Program/Management</td>
<td>Threat Awareness Program</td>
<td>Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.</td>
<td>Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address the concern is for organizations to share threat information including threat events (i.e., tactics, techniques, and procedures) that organizations have experienced; mitigations that organizations have found effective against certain types of threats; and threat intelligence (i.e., indicators and warnings about threats). Threat information sharing may be bilateral or multilateral. Bilateral threat sharing includes government-to-government or government-to-government cooperation. Multilateral threat sharing includes organizations taking part in threat-sharing consortia. Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.</td>
</tr>
<tr>
<td>BA-4, PM-12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PM-18 (1)</td>
<td>2</td>
<td>Program/Management</td>
<td>Automated Threats for Sharing Threat Intelligence</td>
<td>Display automated mechanisms to maximize the effectiveness of sharing threat intelligence information.</td>
<td>To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensor needs to be searching for. By utilizing well established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed into monitoring tools, the relevant threat detection signatures.</td>
</tr>
<tr>
<td>CA-6, PM-10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PM-17</td>
<td>1</td>
<td>Program/Management</td>
<td>Protecting Controlled Unclassified Information on External Systems</td>
<td>a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards.</td>
<td>Controlled unclassified information is defined by the National Archives and Records Administration along with the safeguarding and dissemination requirements for such information and is codified in 32 CFR 2002.19. The policy prescribes the specific use and conditions to be implemented in accordance with organizational procedures, including via its contracting processes.</td>
</tr>
<tr>
<td>CA-6, PM-10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the organization’s privacy program, and:
   1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
   2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; and
   3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
   4. Specifies management commitment, compliance, and the strategic goals and objectives of the privacy program;
   5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and
   6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and
   7. Updates the plan to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

The privacy program plan is a formal document that provides an overview of the organization’s privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the senior agency official for privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the privacy management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be represented in single documents or compilations of documents.

The senior agency official for privacy is responsible for designating which privacy controls the organization will treat as program management, controls, system-specific, and hybrid controls. Privacy program plans provide sufficient information about the privacy program management and common controls (including the specification of parameters and assignment and extension statements explicitly or by reference) to enable control implementation that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended.

Program management controls are generally implemented at the organization level and are essential for managing the organization’s privacy program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular information system. The privacy plans for individual systems and the organization-wide privacy program plan together, provide complete coverage for the privacy controls employed within the organization. Common controls are documented in an appendix to the organization’s privacy program plan unless the controls are included in a separate privacy plan for a system. The organization-wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls.

PM-19 1 Program Management | Privacy Program Leadership Role

Appoint a senior agency official for privacy, with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks throughout the organization-wide privacy program.

The privacy officer is an organizational official. For federal agencies, as defined by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, this official is designated as the senior agency official for privacy. Organizations may also refer to this official as the chief privacy officer. The senior agency official for privacy also has a role in the data management board (see PM-22) and the data integrity board (see PM-26).

PM-20 1 Program Management | Dissemination of Privacy Program Information

Maintain a central resource webpage on the organization’s principal public website that serves as a central source of information about the organization’s privacy program and that:

- Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;
- Ensures that organizational privacy practices and reports are publicly available; and
- Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

Organizations maintain a central resource webpage on their principal public website for their privacy program. For federal agencies, this page is located at www.[agency].gov/privacy. Organizations should use the webpage to inform the public about privacy policies and practices, including privacy impact assessments, system of records notices, computer matching notices and agreements, [PRIVACT] exemption and implementation rules, instructions for individuals making an access or amendment request, privacy reports, privacy policies, email addresses for questions/complaints, blogs, and annual publications.

PM-21 1 Program Management | Accounting of Disclosures

Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

- Date, nature, and purpose of each disclosure; and
- Name and address, or other contact information of the person to or on whose behalf the disclosure was made;
- Time and date of disclosure; and
- Name and address, or other contact information of the person to or on whose behalf the disclosure was made.

Additionally, processes include the provision of responses to individuals of decisions to deny personally identifiable information has been disclosed; to provide a basis for subsequently reviewing organizational compliance with conditions for disclosures. For federal agencies, keeping an accounting of disclosures is required by the [PRIVACT]; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision. Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures along with the required information. Automated mechanisms can be used by organizations to determine when personally identifiable information is disclosed, including commercial services providing certifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statues and policies governing disclosure or dissemination of information and dissemination restrictions.

PM-22 1 Program Management | Personally Identifiable Information Quality Management

Develop and document policies and procedures for:

- Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
- Correcting or deleting inaccurate or outdated personally identifiable information; and
- Disseminating notice of correction or deletion personally identifiable information to individuals or other appropriate entities; and
- Appeals of adverse decisions on correction or deletion requests.

Personally identifiable information quality management include steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information. Organizational policies and procedures for personally identifiable information quality management are important because inaccurate or outdated personally identifiable information maintained by organizations may cause problems for individuals. Organizations consider the quality of personally identifiable information maintained in business functions where inaccurate information may result in adverse decisions or the denial of benefits and services, or the disclosure of the information may cause organizations and individuals to be subject to adverse actions.

Organizations consider creating policies and procedures for the removal of such information. The senior agency official for privacy ensures that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of personally identifiable information, and to appeal adverse decisions concerning the correction or deletion of such information. The senior agency official for privacy also has a role in the data management board (see PM-22) and the data integrity board (see PM-26).
PM-23 1 Program/Management | Data Governance Body
establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].

PM-24 1 Program/Management | Data Integrity Board
Establish a Data Integrity Board to:

- Review proposals to conduct or participate in a matching program; and
- Conduct an annual review of all matching programs in which the agency has participated.

PM-25 1 Program/Management | Minimization of PI Used in Testing, Training, and Research
Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research.

- Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
- Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
- Review and update policies and procedures [Assignment: organization-defined frequency].

PM-26 1 Program/Management | Complaint Management
Develop a process for receiving and responding to complaints, concerns, or questions from individuals about the organization's overarching risk management strategy and can guide and inform the system or system services. The supply chain risk management strategy can be incorporated into the organization's Data Integrity Board and the organization's senior accountable official for privacy, and senior accountable official for risk management.

PM-27 1 Program/Management | Privacy Reporting
Review and update privacy reports [Assignment: organization-defined frequency].

PM-28 1 Program/Management | Risk Framing
Risk framing is most effective when conducted at the organization level. The assumptions, constraints, risk tolerances, priorities, and trade-offs are defined by the organization.

- Identify and document:
  - Assumptions affecting risk assessments, risk responses, and risk monitoring;
  - Constrained affecting risk assessments, risk responses, and risk monitoring;
  - Priorities and trade-offs considered by the organization for managing risk; and
  - Risk responses to complaints, concerns, or questions from individuals within [Assignment: organization-defined time-period]; and
  - Review and update risk framing considerations [Assignment: organization-defined frequency].

PM-29 1 Program/Management | Risk Management Program Leadership Roles
Appoint a Senior Accountability Officer for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgeting planning processes; and

- Establish a Risk Executive Function to view and analyze risks from an organization-wide perspective and ensure management of risk is consistent across the organization.

PM-30 1 Program/Management | Supply Chain Risk Management Strategy
An organization-wide supply chain risk management strategy includes an overall strategy to ensure that the supply chain risk management program is consistent with the organization's overarching risk management strategy and the associated roles and responsibilities. The supply chain risk management includes considerations of system security and privacy risk assessments associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy is incorporated into the organization's Data Integrity Board and the organization's senior accountable official for privacy, and senior accountable official for risk management.

- Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.
- Implement the supply chain risk management strategy consistently across the organization; and
- Establish a Risk Executive Function to view and analyze risks from an organization-wide perspective and ensure management of risk is consistent across the organization.
### PM-01 Personnel Security | Policy and Procedures

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Personnel Security</strong></td>
</tr>
<tr>
<td>2</td>
<td><strong>Position Risk Designation</strong></td>
</tr>
<tr>
<td>3</td>
<td><strong>Personnel Screening</strong></td>
</tr>
<tr>
<td>4</td>
<td><strong>Personal Access and Asset Security</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>Emergency Management</strong></td>
</tr>
<tr>
<td>6</td>
<td>**Personnel Security</td>
</tr>
<tr>
<td>7</td>
<td>**Personnel Security</td>
</tr>
<tr>
<td>8</td>
<td>**Personnel Security</td>
</tr>
</tbody>
</table>

#### PM-01 Personnel Security

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Personnel Security</strong></td>
</tr>
<tr>
<td>2</td>
<td><strong>Position Risk Designation</strong></td>
</tr>
<tr>
<td>3</td>
<td><strong>Personnel Screening</strong></td>
</tr>
<tr>
<td>4</td>
<td><strong>Personal Access and Asset Security</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>Emergency Management</strong></td>
</tr>
<tr>
<td>6</td>
<td>**Personnel Security</td>
</tr>
<tr>
<td>7</td>
<td>**Personnel Security</td>
</tr>
<tr>
<td>8</td>
<td>**Personnel Security</td>
</tr>
</tbody>
</table>

#### PM-01 Personnel Security

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Personnel Security</strong></td>
</tr>
<tr>
<td>2</td>
<td><strong>Position Risk Designation</strong></td>
</tr>
<tr>
<td>3</td>
<td><strong>Personnel Screening</strong></td>
</tr>
<tr>
<td>4</td>
<td><strong>Personal Access and Asset Security</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>Emergency Management</strong></td>
</tr>
<tr>
<td>6</td>
<td>**Personnel Security</td>
</tr>
<tr>
<td>7</td>
<td>**Personnel Security</td>
</tr>
<tr>
<td>8</td>
<td>**Personnel Security</td>
</tr>
</tbody>
</table>

#### PM-01 Personnel Security

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Personnel Security</strong></td>
</tr>
<tr>
<td>2</td>
<td><strong>Position Risk Designation</strong></td>
</tr>
<tr>
<td>3</td>
<td><strong>Personnel Screening</strong></td>
</tr>
<tr>
<td>4</td>
<td><strong>Personal Access and Asset Security</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>Emergency Management</strong></td>
</tr>
<tr>
<td>6</td>
<td>**Personnel Security</td>
</tr>
<tr>
<td>7</td>
<td>**Personnel Security</td>
</tr>
<tr>
<td>8</td>
<td>**Personnel Security</td>
</tr>
</tbody>
</table>
PS-4 1 Personnel Security | Personnel Termination

(a) Upon termination of individual employment:
1. Terminate or revoke any authorizations and credentials associated with the individual;
2. Disable system access within (Assignment: organization-defined time-period);
3. Review and confirm ongoing operational need for current logical and physical access authorizations to organizational information; and
4. Review and update the access agreements [Assignment: organization-defined frequency].
(b) If the individual had system privileges within [Assignment: organization-defined time-period following the formal transfer action];
1. Notify [Assignment: organization-defined personnel or roles] within (Assignment: organization-defined time-period);
2. Review and update the access agreements [Assignment: organization-defined frequency]; and
3. Conduct exit interviews that include a discussion of [Assignment: organization-defined topics];
(c)gd. If the individual had system privileges within [Assignment: organization-defined time-period];
1. Require external providers to comply with personnel security policies and procedures established by the organization;
2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].
(d) If the individual had system privileges within [Assignment: organization-defined time-period];
1. Develop and document access agreements for organizational systems;
2. Review and update the access agreements [Assignment: organization-defined frequency]; and
3. Notify appropriate stakeholders regarding matters of employee sanctions.

Notes
PT-2 1 (PT-4) PII Processing and Transparency | Authority to Process Personally Identifiable Information

a. Determine and document the assignment: organization-defined authority[1] that permits the assignment: organization-defined processing[2] of personally identifiable information[3]; and
b. Restrict the assignment: organization-defined processing[2] of personally identifiable information to only that which is authorized.

- Processing of personally identifiable information is an operation or set of operations that the organization performs with respect to personally identifiable information throughout the information life cycle. Processing includes, but is not limited to, creation, collection, holding, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include aging, generation, and transformation, as well as analysis techniques, such as sorting.
- The purpose of processing personally identifiable information refers to the intended purpose or expected result of the processing activity and is fundamental to determining the necessity of the processing activity for the organization. Processing is necessary to accomplish the purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

PT-2 (1) PII Processing and Transparency | Authority to Process Personally Identifiable Information | Data Tagging


- Data tags support tracking and enforcement of authorized processing by conveying the types of processing that are authorized along with the relevant elements of personally identifiable information throughout the system. Data tags may also support the use of automated tools.

PT-2 (2) PII Processing and Transparency | Authority to Process Personally Identifiable Information | Automation

- Message enforcement of the authorized processing of personally identifiable information using assignment: organization-defined automated mechanisms.

- Automated mechanisms augment verification that only authorized processing is occurring.


a. Identify and document the assignment: organization-defined authority[2] for processing personally identifiable information[3];

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the assignment: organization-defined processing of personally identifiable information to only that which is compatible with the identified purpose[2]; and

d. Monitor changes in processing personally identifiable information and implement assignment: organization-defined mechanisms[3] to ensure that any changes are made in accordance with assignment: organization-defined requirements.

- Organizations should consider applicable requirements and organizational policies to determine how to document the authority for Federal agencies. The authority to process personally identifiable information is documented in privacy policies and notices, system of records notices, privacy impact assessments, [PRIVACT] statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

- Organizations take steps to ensure that personally identifiable information is processed only for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring and auditing organizational use of personally identifiable information.

PT-3 (1) PII Processing and Transparency | Personally Identifiable Information Processing Purposes | Data Tagging

- Attach data tags containing the following purposes to assignment: organization-defined elements of personally identifiable information[3]:

- Data tags support tracking of processing purposes by conveying the types of processing purposes that are authorized along with the relevant elements of personally identifiable information throughout the system. By conveying the processing purposes in a data tag along with the personally identifiable information to the information processor or system owner or operator, the data processor or system owner or operator can identify whether a change in processing would be compatible with the identified and documented purpose(s).

- Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly the organization in subject to multiple jurisdictions or sources of authority. For organizations whose processing is not determined according to legal authorities, the organization’s policies and determinations govern how the processing personally identifiable information. While processing of personally identifiable information may be highly permissible, privacy risks may still arise from its processing. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks.

- Organizations consider applicable requirements and organizational policies to determine how to document the authority for processing. The authority to process personally identifiable information is documented in public privacy notices and notices, system of records notices, privacy impact assessments, [PRIVACT] statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

- Organizations take steps to ensure that personally identifiable information is processed only for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring and auditing organizational use of personally identifiable information.

PT-4 1 (PT-8, RA-4, SI-12, SI-18) PII Processing and Transparency | Minimization

b. Describe the purpose(s) in the public privacy notices and policies of the organization;
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Document</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT-6</td>
<td>1</td>
<td>Implement (Assignment: organization defined tools or mechanisms) for individuals to consent to the processing of their personally identifiable information prior to its collection:</td>
<td>Permission allows individuals to participate in the decision-making about the processing of their information and transfers some of the risk that arises from the processing of personally identifiable information from the organization to an individual. Organizations consider whether other controls may more effectively mitigate privacy risks either alone or in conjunction with consent. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting this control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks arising from their authorization. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the data actions carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanisms for obtaining consent, including how to properly authenticate and identify proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.</td>
<td>AC-10, PT-4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-6 (1)</td>
<td>2</td>
<td>Provide (assignment: organization defined mechanisms) to allow individuals to tailor processing permissions to selected elements of personally identifiable information</td>
<td>Consent enables individuals to participate in how their personally identifiable information is being processed at the time when such participation may be most useful to the individual. Individuals can use these permissions to tailor processing requests to their preference for information both collected in plain language and avoiding technical jargon. Consent may be provided by general consent mechanisms, such as the use of a single blanket consent, or by presenting just-in-time notice to individuals in conjunction with data actions that require consent. In some cases, organizations may provide a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.</td>
<td>PT-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-6 (2)</td>
<td>2</td>
<td>Provide (assignment: organization defined mechanisms) to allow individuals to tailor processing permissions to selected elements of personally identifiable information</td>
<td>Consent enables individuals to participate in how their personally identifiable information is being processed at the time when such participation may be most useful to the individual. Organizations consider whether other controls may more effectively mitigate privacy risks either alone or in conjunction with consent. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting this control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks arising from their authorization. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the data actions carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanisms for obtaining consent, including how to properly authenticate and identify proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.</td>
<td>PT-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-6 (3)</td>
<td>2</td>
<td>Provide (assignment: organization defined mechanisms) to allow individuals to tailor processing permissions to selected elements of personally identifiable information</td>
<td>Consent enables individuals to participate in how their personally identifiable information is being processed at the time when such participation may be most useful to the individual. Organizations consider whether other controls may more effectively mitigate privacy risks either alone or in conjunction with consent. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting this control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks arising from their authorization. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the data actions carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanisms for obtaining consent, including how to properly authenticate and identify proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.</td>
<td>PT-2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**

- PM-21
- PM-22, PT-2, PT-5, PT-6, RA-1, SI-18
- PT-6
<table>
<thead>
<tr>
<th>Central ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Question</th>
<th>Document</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT-7</td>
<td>1</td>
<td>[PRIVACY] Processing and Transparency</td>
<td>System of Records</td>
<td>Notice</td>
<td>our systems that process information that will be maintained in a PRIVACY Act system of records:</td>
<td>The [PRIVACY] Act requires that federal agencies publish a system of records notice to the Federal Register upon the establishment and/or modification of a [PRIVACY] Act system of records. As a general matter, a system of records notice is required when an agency maintains a group of any records under the control of the agency from which the system is established or is maintained that is retrieved by the name of an individual or by some identifying number, symbol, or other identifier. The notice describes the existence and character of the system, and identifies the system of records, the purpose(s) of the system, the authority for maintenance of the system, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in OMAA’s (98).</td>
<td>FM-20, PT-2, PT-3, PT-4</td>
<td></td>
</tr>
<tr>
<td>PT-7(11)</td>
<td>2</td>
<td>[PRIVACY] Processing and Transparency</td>
<td>System of Records</td>
<td>Notice</td>
<td>Routine Uses: Review all routine uses published in the system of records notice as [Assignment: organization-defined frequency] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.</td>
<td>The [PRIVACY] Act requires a periodic review of the routine uses of a system of records. The review must be a periodic review that is conducted at least once every year or once every two years, as the agency determines, to ensure continued accuracy, and to ensure that periodic uses continue to be compatible with the purpose for which the information was collected.</td>
<td>PT-2, PT-3</td>
<td></td>
</tr>
<tr>
<td>PT-7(12)</td>
<td>2</td>
<td>[PRIVACY] Processing and Transparency</td>
<td>System of Records</td>
<td>Notice</td>
<td>Exemption Rules: Review all Privacy Act exemptions claimed for the system of records as [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law, and that they have been promulgated as regulations, and that they are accurately described in the system of records notice.</td>
<td>The [PRIVACY] Act requires a periodic review of the Privacy Act exemptions claimed for a system of records. The review must be a periodic review that is conducted at least once every year or once every two years, as the organization determines, to ensure that they remain appropriate and necessary in accordance with law, and that they have been promulgated as regulations, and that they are accurately described in the system of records notice.</td>
<td>PT-2, PT-3</td>
<td></td>
</tr>
<tr>
<td>PT-8(11)</td>
<td>2</td>
<td>[PRIVACY] Processing and Transparency</td>
<td>Specific Categories</td>
<td>of Personally Identifiable Information</td>
<td>Social Security Number</td>
<td>When a system processes Social Security numbers: (a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier; (b) Do not store any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; (c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statute or other authority such number is collected, and what use will be made of it.</td>
<td>Federal law and policy establish specific requirements for organizations' processing of Social Security numbers. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information, and observe any particular requirements that apply.</td>
<td>None. (Related Controls: The [PRIVACY] Act limits agencies' ability to process information that describes how individuals exercise rights guaranteed by the First Amendment. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary. )</td>
</tr>
<tr>
<td>PT-8(12)</td>
<td>2</td>
<td>[PRIVACY] Processing and Transparency</td>
<td>Specific Categories</td>
<td>of Personally Identifiable Information</td>
<td>First Amendment Information</td>
<td>Provide the processing of individual information that is authorized by statute or by the individual or unless pertinent to and within the scope of an otherwise authorized law enforcement activity.</td>
<td>None. (Related Controls: The [PRIVACY] Act limits agencies' ability to process information that describes how individuals exercise rights guaranteed by the First Amendment. Organizations consult with the senior agency official for privacy and legal counsel regarding these requirements.)</td>
<td>None.</td>
</tr>
<tr>
<td>PR-9</td>
<td>1</td>
<td>[PRIVACY] Processing and Transparency</td>
<td>Computer Matching Requirements</td>
<td>When a system organizes personal information for the purpose of conducting a matching program:</td>
<td>Independently verify the information provided by the matching program before taking adverse action against an individual, if required; and, If an individual with notice and an opportunity to contest the findings before taking adverse action against an individual.</td>
<td>The [PRIVACY] Act establishes a set of requirements for federal and non-federal agencies when they engage in a matching program. In general, a matching program is a computerized comparison of records from two or more automated systems of records, or an automated system of records and automated records maintained by a non-federal agency or entity. A matching program involves not just the matching activity itself, but also the investigative follow-up and ultimate action, if any.</td>
<td>FM-24</td>
<td></td>
</tr>
<tr>
<td>RA-0</td>
<td>0</td>
<td>Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td>This control addresses policy and procedures for the controls in the RA Family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate in their development. Security and privacy programs and policies at the organization level are preferable, in general, and may be delegated to the need for systemspecific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Remaining controls does not constitute an organizational policy or procedure.</td>
<td>None. (Related Controls: RA-9, RA-10. )</td>
<td></td>
</tr>
</tbody>
</table>

Page 63 of 108
RA-2 (1) 2 Risk Assessment | Security Categorization | Impact-level Prioritization

Execute an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.

Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individually, other organizations, and the Nation based on the operation and use of systems. Risk assessments also consider risk from external parties, including individuals accessing organizational systems; contractors operating systems on behalf of the organization; service providers; and outsourcing entities.

Organizations can conduct risk assessments at all three levels of the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can be conducted at various steps in the Risk Management Framework, including categorization, control selection, control implementation, control assessment, system authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

In addition to the information processed, stored, and transmitted by the system, risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and other supply chain-related information or artifacts. Assessments of risk can play an important role in control selection, design, the intended use of the system, testing results, and other supply chain-related information or artifacts. Assessments of risk can play an important role in control selection, design, the intended use of the system, testing results, and other supply chain-related information or artifacts.

RA-3 (1) 1 Risk Assessment | Risk Assessment

Conduct a risk assessment, including:

1. The likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, and transmits; and the information derived from the system.
2. The likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.
3. The likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, and transmits; and the information derived from the system; and
4. Develop a risk assessment plan that includes an identification of organizational assets to be assessed; and
5. Develop a risk management plan that identifies the organizational resources that must be protected; and
6. Identify the organizational assets that must be protected.

RA-3 (2) 2 Risk Assessment | Risk Assessment | Supply Chain Risk Assessment

[2] Assess supply chain risks associated with [assignment: organization-defined systems, system components, and system versions], and
[3] Update the supply chain risk assessment [assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Supply chain-related events include disruption, use of defective components, inventory of counterfeit, theft, malicious development practices, improper delivery practices, and inventory of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and therefore can also adversely impact organizational operations (including mission, function, image, or reputation); organizational assets, individuals, other organizations, and the Nation. The supply chain-related events can be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.
Level | Discussion
--- | ---
Risk Assessment | Risk Assessment Update
Withdrawn | Control Name
X | RA-4 | AU-11
Risk Assessment | Predictive Cyber Analytics
Identify the following advanced automation and analytics capabilities to predict and identify risks:
- Assignment: organization-defined automatic and analytics capabilities.

A property security operations center (SOC) or Computer Incident Response Team (CIRT) may be augmented by the volume of information generated by the proliferation of security tools and appliances. An enterprise-automated analytics and analytics to detect and respond to anomalies based on the scale and volume of data generated by security tools and appliances.

Control Name
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
X | Withdrawn: Incorporated into CM-8 | RA-5 1 Risk Assessment | Risk Assessment Update | Predictive Cyber Analytics
RA-6 1 Risk Assessment | Technical Surveillance Countermeasures Survey

Employ a technical surveillance countermeasures survey at [Assignment: organization-defined locations]. [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators]].

A technical surveillance countermeasures survey is a service provided by qualified personnel to detect the presence of technical surveillance devices and hazards and to identify technical security weaknesses that could be used in the conduct of technical penetration of the surveyed facility. Technical surveillance countermeasures surveys also provide evaluations of the technical security posture of organizations and facilities and include visual, electronic, and physical examinations of surveyed facilities, internally and externally. The surveys also provide useful input for risk assessments and information regarding organizational exposure to potential adversaries.

RA-7 1 Risk Assessment | Risk Response

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

RA-8 1 Risk Assessment | Privacy Impact Assessments

Conduct privacy impact assessments for systems, programs, or other activities before a. Developing or procuring information technology that processes personally identifiable information; and b. Employing the threat hunting capability [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators].

A privacy impact assessment is an analysis of how personally identifiable information is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A privacy impact assessment is both an analytic and a formal document that outlines the privacy and security concerns, legal requirements, and organizational policies and objectives.

Organizations conduct and develop a privacy impact assessment with sufficient detail and specificity to demonstrate that the organization fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the organization’s activity and throughout the information life cycle. In order to conduct a meaningful privacy impact assessment, the organization’s privacy officer or lead privacy officer, in collaboration with program managers, system owners, information technology experts, security officials, counsel, and other relevant organization personnel, must conduct an assessment. A privacy impact assessment is not a time-restricted activity that is limited to the life cycle of the information system or personally identifiable information life cycle. Rather, the privacy analyst continues throughout the system and personally identifiable information life cycle. Accordingly, a privacy impact assessment is a living document that organizes update whenever changes to the information technology, changes to the organization’s practices, or other factors alter the privacy risk associated with the use of such information technology. To conduct the privacy impact assessment, organizations can use security and privacy risk assessments. Organizations may also use other related processes which may have different labels, including privacy threshold analyses. A privacy impact assessment can also serve as notice to the public regarding the organization’s practices with respect to privacy. Although conducting and publishing privacy impact assessments may be required by law, organizations may develop such policies in the absence of applicable law. For federal agencies, privacy impact assessments may be required by [EGOV]; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

RA-9 1 Risk Assessment | Criticality Analysis

Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services]; [Assignment: organization-defined decision points in the system development lifecycle].

Criticality analysis is a key tool for, for example, supply chain risk management, and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive order regulations, directives, policies, and standards; system functionality requirements; system and component interfaces; and system and component dependencies. System owners conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system; decomposition into the specific functions to perform those missions; and translatability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connection to and dependence on cyber physical systems, devices, system of systems, and outsourcing [IVISs]. System components that do not unconditionally access critical system components or functions are considered critical due to the inherent vulnerabilities such components carry. Component and function criticality can assessed in terms of the impact of a system component or function on the mission of the system or by a risk assessment process of the system. System owners determine the criticality of each component and function by risk assessment, by prioritizing the criticality of components and functions, and by reviewing the system’s impact on the mission. Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development lifecycle, organizations may be able to modify the system design to reduce the critical mass of these components and functions, for example, by adding redundancies or alternative paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is as important consideration. Such analysis is conducted as part of security categorization in RA-2.

RA-10 1 Risk Assessment | Threat Hunting

a. Gather and maintain a cyber threat hunting capability to: i. Search for indicators of compromise in organizational systems; and ii. Detect, track, and disrupt threats that evade existing controls; and b. Employ the threat hunting capability [Assignment: organization-defined frequency].

Threat hunting is an active means of cyber defense in contrast to the traditional prevention measures such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandbox, and forensic analysis and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting team leveraging existing threat intelligence may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.

SA 0 System and Service Acquisition

a. Establish and maintain a cyber threat hunting capability to: i. Search for indicators of compromise in organizational systems; and ii. Detect, track, and disrupt threats that evade existing controls; and b. Employ the threat hunting capability [Assignment: organization-defined frequency].

Threat hunting is an active means of cyber defense in contrast to the traditional prevention measures such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandbox, and forensic analysis and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting team leveraging existing threat intelligence may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.
SA-2 1 System and Services Acquisition / Allocation of Resources

This control addresses policy and procedures for the controls in the SA family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy policy and procedures at the organization level are preferable, in general, and may obviate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Policies can be established for security and privacy programs for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Retaining controls does not constitute an organizational policy or procedure.

PM-6, PA-9, SA-8, SA-12

SA-2 2 System and Services Acquisition / System Development Life Cycle

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning; and
b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and
c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

SA-3 1 (2) System and Services Acquisition / System Development Life Cycle / Manage Preproduction Environment

Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.

The preproduction environment includes development, test, and integration environments. The program protection planning processes established by the Department of Defense is an example of managing the preproduction environment for defense contractors. Criticality analysis and the application of controls on developers also contribute to a more secure system development environment.

CM-2, CM-4, RK-2, RK-6, LR-4

SA-3 1 (3) System and Services Acquisition / System Development Life Cycle / Use of Live or Operational Data

a. Apprise, document, and control the use of live data in preproduction environments for the system, system component, or system service; and
b. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data used within the preproduction environments.

Live data is also referred to as operational data. The use of live or operational data is preproduction (i.e., development, test, and integration) environments can result in significant risk to organizations. In addition, the use of personally identifiable information in testing, research, and training increases risk of unauthorized disclosure or misuse of such information. Thus, it is important for the organization to manage any additional risks that may result from use of live or operational data. Organizations can minimize such risk by acting fast or being data driven during the design, development, and testing of systems, system components, and system services. Risk assessment techniques may be used to determine if the risk of using live or operational data is acceptable.

NI-20, SA-2

SA-3 1 (5) System and Services Acquisition / System Development Life Cycle / Technology Refresh

Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.

Technology refresh planning may encompass hardware, software, firmware, protocols, personnel skills sets, suppliers, system providers, and facilities. The use of obsolete or obsolescent technology may increase security and privacy risks associated with, for example, unsupervised components, components unable to implement security or privacy requirements, counterfeit or re-purposed components, slow or inoperable components, components from untrusted sources, untrusted personnel error, or increased complexity. Technology refresh typically occurs during the operation and maintenance stages of the system development life cycle.
SA-4 (5) 2  System and Services Acquisition / Acquisition Process
Functional Properties of Controls

SA-4 (5) 2  System and Services Acquisition / Acquisition Process
Design and Implementation Information for Controls

SA-4 (5) 2  System and Services Acquisition / Acquisition Process
Development Methods, Techniques, and Practices

SA-4 (5) 2  System and Services Acquisition / Acquisition Process
Assignment of Component to Systems

SA-4 (5) 2  System and Services Acquisition / Acquisition Process
System, Component, and Service Configurations

SA-4 (5) 2  System and Services Acquisition / Acquisition Process
Use of Information Assurance Products

SA-4 (5) 2  System and Services Acquisition / Acquisition Process
Unapproved Protection Profiles

SA-4 (5) 2  System and Services Acquisition / Acquisition Process
Continuous Monitoring Flex for Controls

Security and privacy functional requirements are typically crafted from the high-level security and privacy requirements described in SA-2. The derived requirements for low-level and process design methods (e.g., functional properties, systems, functions, and mechanisms) include degree of correctness, completeness, resistance to tampering or replay, and mechanisms to detect attack. Assurance requirements include development practices, procedures, practices, and methodologies; and the evidence from development and assessment activities providing proofs for confidence that the required functionality is implemented and possesses the required strength of mechanism. [SP 800-160 v4] describes the process of requirements engineering as part of the system development life cycle.

Controls can be viewed as descriptions of the safeguards and protections capable for achieving the particular security and privacy objectives of the administration and reducing the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical aspects, administrative aspects, and physical aspects. In some cases, the selection and implementation of a control may require additional specification by the organization in the form of derived requirements or contextual control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.

Security and privacy documentation requirements add all stages of the system development life cycle, the product development life cycle, and the assessment life cycle to determine if the planned, required, and implemented controls meet the level of assurance and the level of assurance is demonstrated. Controls are implemented in a tiered fashion that addresses security and privacy assurance needs of stakeholders. Controls can include technical aspects, administrative aspects, and physical aspects. In some cases, the selection and implementation of a control may require additional specification by the organization in the form of derived requirements or contextual control parameter values.

Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, function, or mechanism) utilized at the interface of the controls and specifically exclude functionality and data structures inherent to the operation of the controls. Organizations may require different levels of detail in the documentation for the design and implementation for controls in organizational systems, system components, or system services based on mission and business requirements; requirements for compliance and trustworthiness; and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can consist of one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-related functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-related functionality. Design and implementation documentation can include: source code, hardware schematics, and the like referred to as the implementation representation of the system.

The objectives of continuous monitoring plans is to determine if the planned requirements have been met and implement continuous monitoring for systems, system components, or system services. Continuous monitoring plans can include frequency of control implementation, the capability to detect control failures, the capability to determine the severity of the latent errors within systems, system components, and system services. Transparency in the methods developers select and implement for systems engineering, systems security and privacy engineering, software development, component and system assessments, and quality control processes is an increased level of assurance in the trustworthiness of the system, system component, or system service being acquired.

The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-related functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-related functionality. Design and implementation documentation can include: source code, hardware schematics, and the like referred to as the implementation representation of the system.
### OCCM Control Set for NIST SP 800-53 rev. 5 Final Public Draft

#### Control Identification (ID) and Level

<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Description</th>
<th>Withdrawn/Incorporated Notes</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-4 (B)</td>
<td>2</td>
<td>System and Services Acquisition / Acquisition Process</td>
<td>Identify the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.</td>
<td>Withdrawn: Incorporated into CM-11, SI-7</td>
<td>CM-3, SA-9</td>
<td></td>
</tr>
<tr>
<td>SA-4 (B)</td>
<td>2</td>
<td>System and Services Acquisition / Acquisition Process</td>
<td>Use only information technology products on the FIPS 201 approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.</td>
<td>Products on the FIPS 201 approved products list must meet PIV requirements for Personal Identity Verification (PIV) at Federal Government Contractors. For PIV cards issued for applications other than Federal Government Contractors, the PIV Product list must be used.</td>
<td>SA-4 (9)</td>
<td></td>
</tr>
<tr>
<td>SA-4 (B)</td>
<td>2</td>
<td>System and Services Acquisition / Acquisition Process</td>
<td>Include (assignment: organization-defined Privacy Act requirements) in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.</td>
<td>Include [Assignment: organization-defined Privacy Act requirements] in the acquisition contract for the operation of a system of records to accomplish an organizational mission or function, the organization, consistent with its authority, causes the requirement of the (FIPS-207) to be applied to the system of records.</td>
<td>SA-4 (9), SA-9, SA-10, SA-11, SI-13, SI-17, SI-12, SI-3</td>
<td></td>
</tr>
<tr>
<td>SA-5 (1)</td>
<td>2</td>
<td>System and Services Acquisition / System Documentation</td>
<td>Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: (Assignment: organization-defined systems security and privacy engineering principles).</td>
<td>Systems security and privacy engineering principles are closely related to and are implemented throughout the system development life cycle (see SA-4). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduce the susceptibility to disruptions, hazards, threats, and creating privacy problems for individuals. Examples of systems security engineering principles include: developing layered protections, establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; defining physical and logical security boundaries; ensuring that developers are trained on how to build secure software; taking controls to meet organizational needs; performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and services; reduce risk to acceptable levels; and make informed risk management decisions. System security engineering principles can also be used to protect against certain supply chain risks including incursion and tamper-resistant hardware into a design.</td>
<td>CM-3, CM-4, CM-5, CM-7</td>
<td></td>
</tr>
<tr>
<td>SA-5 (1)</td>
<td>2</td>
<td>System and Services Acquisition / System Documentation</td>
<td>Document attempts to obtain system, system component, or service documentation when such documentation is either unavailable or nonexistent and taken (Assignment: organization-defined actions) in response.</td>
<td>When an organization provides a contract for the operation of a system of records to accomplish an organizational mission or function, the organization, consistent with its authority, causes the requirement of the (FIPS-207) to be applied to the system of records.</td>
<td>SA-4 (9), SA-9, SA-10, SA-11, SI-13, SI-17, SI-12, SI-3</td>
<td></td>
</tr>
<tr>
<td>SA-5 (1)</td>
<td>2</td>
<td>System and Services Acquisition / System Documentation</td>
<td>Record attempts to obtain system, system component, or service documentation when such documentation is either unavailable or nonexistent and taken (Assignment: organization-defined actions) in response.</td>
<td>When an organization provides a contract for the operation of a system of records to accomplish an organizational mission or function, the organization, consistent with its authority, causes the requirement of the (FIPS-207) to be applied to the system of records.</td>
<td>CM-3, CM-4, CM-5, CM-7, CM-9, CM-12, CM-13, CM-15, CM-16, CM-17, SI-23, SI-22, SI-19, SI-2, SI-5, SI-6</td>
<td></td>
</tr>
<tr>
<td>SA-5 (1)</td>
<td>2</td>
<td>System and Services Acquisition / System Documentation</td>
<td>Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.</td>
<td>The identification of functions, ports, protocols, and services early in the system development life cycle, for example, during the initial requirements definition and design stages, allows organizations to influence the design of the system, system component, or system service. This early involvement in the system life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or when requiring system service providers to do so: Early identification of functions, ports, protocols, and services avoids costly rectifying controls after the system, system component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.</td>
<td>SA-8, SA-9, SA-10, SA-11, SI-13, SI-17, SI-12, SI-3</td>
<td></td>
</tr>
<tr>
<td>SA-8 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Acquisition Process</td>
<td>Use only information technology products on the FIPS 201 approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.</td>
<td>Products on the FIPS 201 approved products list must meet PIV requirements for Personal Identity Verification (PIV) at Federal Government Contractors. For PIV cards issued for applications other than Federal Government Contractors, the PIV Product list must be used.</td>
<td>SA-8 (9), SA-9, SA-10, SA-11, SI-13, SI-17, SI-12, SI-3</td>
<td></td>
</tr>
<tr>
<td>SA-8 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Acquisition Process</td>
<td>Use only information technology products on the FIPS 201 approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.</td>
<td>Products on the FIPS 201 approved products list must meet PIV requirements for Personal Identity Verification (PIV) at Federal Government Contractors. For PIV cards issued for applications other than Federal Government Contractors, the PIV Product list must be used.</td>
<td>SA-8 (9), SA-9, SA-10, SA-11, SI-13, SI-17, SI-12, SI-3</td>
<td></td>
</tr>
<tr>
<td>SA-8 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Acquisition Process</td>
<td>Use only information technology products on the FIPS 201 approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.</td>
<td>Products on the FIPS 201 approved products list must meet PIV requirements for Personal Identity Verification (PIV) at Federal Government Contractors. For PIV cards issued for applications other than Federal Government Contractors, the PIV Product list must be used.</td>
<td>SA-8 (9), SA-9, SA-10, SA-11, SI-13, SI-17, SI-12, SI-3</td>
<td></td>
</tr>
</tbody>
</table>

### Summary

The OCCM Control Set for NIST SP 800-53 rev. 5 Final Public Draft contains controls related to systems security and privacy engineering principles. These principles help organizations develop trustworthy, secure, and resilient systems and reduce the susceptibility to disruptions, hazards, threats, and privacy problems for individuals. The controls focus on identifying, acquiring, and documenting systems, system components, and system services to ensure that they are designed with security and privacy in mind from the outset. Organizations are encouraged to apply these principles throughout the system development life cycle, including during the initial requirements definition and design stages. This approach helps ensure that security and privacy are integrated into the system design and development at a time when changes can be made more easily and cost-effectively. The controls also address the need for clear documentation of security and privacy features and mechanisms, and for ensuring that these features are effective and understood by users and system owners. The overall goal is to create systems that are secure by design, reducing the risk of vulnerabilities and unauthorized access.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-8 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td>Withdrawn</td>
<td>Implement the security design principle of least common mechanism.</td>
<td>The principle of least common mechanism states that the amount of mechanism common to more than one user and depend on by all users is minimized. Mitigation of mechanism implies that different components of a system refrain from using the same mechanism to access system resources. Every shared mechanism (exclusively a mechanism involving shared variable) represents a potential information path between users and is designed with great care to use it does not unnecessarily compartmentalize security. (SA-2.2.2.7). Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing system state among different programs. A single program accessing a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels.</td>
<td>SC-2, SC-3</td>
<td></td>
</tr>
<tr>
<td>SA-8 (2)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td>Least Common Mechanism</td>
<td>Implement the security design principle of least common mechanism in (Assignment: organization-defined systems or system components).</td>
<td>The principle of least common mechanism states that the amount of mechanism common to more than one user and depend on by all users is minimized. Mitigation of mechanism implies that different components of a system refrain from using the same mechanism to access system resources. Every shared mechanism (exclusively a mechanism involving shared variable) represents a potential information path between users and is designed with great care to use it does not unnecessarily compartmentalize security. (SA-2.2.2.7). Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing system state among different programs. A single program accessing a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels.</td>
<td>SC-2, SC-3</td>
<td></td>
</tr>
<tr>
<td>SA-8 (3)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td>Least Common Mechanism</td>
<td>Implement the security design principle of least common mechanism in (Assignment: organization-defined systems or system components).</td>
<td>The principle of least common mechanism states that the amount of mechanism common to more than one user and depend on by all users is minimized. Mitigation of mechanism implies that different components of a system refrain from using the same mechanism to access system resources. Every shared mechanism (exclusively a mechanism involving shared variable) represents a potential information path between users and is designed with great care to use it does not unnecessarily compartmentalize security. (SA-2.2.2.7). Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing system state among different programs. A single program accessing a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels.</td>
<td>SC-2, SC-3</td>
<td></td>
</tr>
<tr>
<td>SA-8 (4)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td>Least Common Mechanism</td>
<td>Implement the security design principle of least common mechanism in (Assignment: organization-defined systems or system components).</td>
<td>The principle of least common mechanism states that the amount of mechanism common to more than one user and depend on by all users is minimized. Mitigation of mechanism implies that different components of a system refrain from using the same mechanism to access system resources. Every shared mechanism (exclusively a mechanism involving shared variable) represents a potential information path between users and is designed with great care to use it does not unnecessarily compartmentalize security. (SA-2.2.2.7). Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing system state among different programs. A single program accessing a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels.</td>
<td>SC-2, SC-3</td>
<td></td>
</tr>
<tr>
<td>SA-8 (5)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td>Least Common Mechanism</td>
<td>Implement the security design principle of least common mechanism in (Assignment: organization-defined systems or system components).</td>
<td>The principle of least common mechanism states that the amount of mechanism common to more than one user and depend on by all users is minimized. Mitigation of mechanism implies that different components of a system refrain from using the same mechanism to access system resources. Every shared mechanism (exclusively a mechanism involving shared variable) represents a potential information path between users and is designed with great care to use it does not unnecessarily compartmentalize security. (SA-2.2.2.7). Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing system state among different programs. A single program accessing a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels.</td>
<td>SC-2, SC-3</td>
<td></td>
</tr>
<tr>
<td>SA-8 (6)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td>Least Common Mechanism</td>
<td>Implement the security design principle of least common mechanism in (Assignment: organization-defined systems or system components).</td>
<td>The principle of least common mechanism states that the amount of mechanism common to more than one user and depend on by all users is minimized. Mitigation of mechanism implies that different components of a system refrain from using the same mechanism to access system resources. Every shared mechanism (exclusively a mechanism involving shared variable) represents a potential information path between users and is designed with great care to use it does not unnecessarily compartmentalize security. (SA-2.2.2.7). Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing system state among different programs. A single program accessing a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels.</td>
<td>SC-2, SC-3</td>
<td></td>
</tr>
<tr>
<td>SC-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].

The principle of reduced complexity states that the system design is as simple and small as possible. A small and simple design is more understandable, more explainable, and less prone to error. The reduced complexity principle applies to any aspect of a system, but it has particular importance for security due to the various employees performed to obtain evidence about the emergent security property of the system. For such analysis to be successful, a small and simple design is essential. Application of the principle of reduced complexity contributes to the ability of system developers to understand the correctness and completeness of system security functions. It also facilitates identification of potential vulnerabilities. The corollary of reduced complexity states that the simplicity of the system is directly related to the number of vulnerabilities it will contain—i.e., simpler systems contain fewer vulnerabilities. An important benefit of reduced complexity is that it is easier to understand whether the trusted security policy has been captured in the system design, and that fewer vulnerabilities are likely to be introduced during engineering development. An additional benefit is that it is much easier to conclude about correctness, completeness, and existence of vulnerabilities that can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex. Transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6) may require implementing the older and newer technologies simultaneously during the transition period. This may result in a temporary increase in system complexity during the transition.

SA-8 (A) 2 System and Services Acquisition / Security and Privacy Engineering Principles | Secure Evolvability

Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].

The principle of secure evolvability states that a system is developed to facilitate the maintenance of its security properties when there are changes to the system's structure, interfaces, interactions (i.e., system architecture), functionality, or its configuration (i.e., security policy enforcement). Changes include a new, an enhanced, or an upgraded system capability, maintenance and sustainment activities, and reconfiguration. Although it is not possible to plan for every aspect of system evolution, system upgrades and changes can be anticipated by analyses of mission or business strategic objectives, anticipated changes in the threat environment, and anticipated maintenance and sustainment needs. It is unrealistic to expect that complex systems remain secure in contexts not envisioned during development, whether such contexts are related to the operational environment or to usage. A system may be secure in some new contexts, but there is no guarantee that its emergent behavior will always be secure. It is easier to build trustworthy into a system from the outset, and it follows that the sustainment of system trustworthiness requires planning for change as opposed to adapting in an ad hoc or non-systematic manner. The benefits of this principle include reduced life-cycle costs; reduced cost of ownership; improved system security; more effective management of security risk; and less risk uncertainty.

SA-8 (A) 2 System and Services Acquisition / Security and Privacy Engineering Principles | Trusted Components

Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].

The principle of trusted components states that a component is trustworthy to the extent that it is a trust commensurate with the security dependencies it supports, i.e., how much it is trusted to perform its security functions by other components. This principle enables the composition of components such that trustworthiness is not inadvertently diminished and where consequently the trust is not misplaced. Ultimately this principle demands some metric by which the trust is a component and the trustworthiness of a component can be measured on the same abstract scale. The principle of trusted components is particularly relevant when considering systems and components in which there are complex chains of trust dependencies. A trust dependency is also referred to as a trust relationship and there may be chains of trust relationships. The principle of trusted components also applies to a compound component that consists of subcomponents (e.g., a subject), which may have varying levels of trustworthiness. The conservative assumption is that the trustworthiness of a compound component is at least the least trustworthy component. It may be possible to provide a security engineering rationale that the trustworthiness of a particular compound component is greater than the conservative assumption, however, such rationale reflects logical reasoning based on a clear statement of the trustworthiness objectives, and relevant and credible evidence. The trustworthiness of a compound component is not the same as increased application of defense-in-depth techniques within the component, or replacement of components. Defense-in-depth techniques do not increase the trustworthiness of the whole above that of the least trustworthy component.

SA-8 (A) 2 System and Services Acquisition / Security and Privacy Engineering Principles | Hierarchical Trust

Implement the security design principle of hierarchical trust in [Assignment: organization-defined systems or system components].

The principle of hierarchical trust for components builds on the principle of trusted components and states that the security dependencies in a system will form a partial ordering if they preserve the principle of trusted components. The partial ordering provides the basis for trustworthiness reasoning or providing an assurance case or argument when comparing a secure system from heterogeneous trustworthy components. To analyze a system composed of heterogeneous trustworthy components for its trustworthiness, it is essential to eliminate circular dependencies with regard to the trustworthiness. If more trustworthy component located in a lower layer of the system were to depend upon a less trustworthy component in a higher layer, this would be effect, but the components in the same "less trustworthy" equivalence class per the principle of trusted components. Trust relationships, or chains of trust, can have various interpretations. For example, the root certificate of a certificate hierarchy is the most trusted node in the hierarchy, whereas the leaves in the hierarchy may be the least trusted nodes. Another example occurs in a layered high-assurance system where the security kernel (including the hardware-based, which is located at the lowest layer of the system, is the most trustworthy component. The principle of hierarchical trust, however, does not prohibit the use of semi-trustworthy components. There may be cases in a system of low-trustworthiness, where it is reasonable to employ a highly trustworthy component rather than one that is less trustworthy (e.g., due to availability or other cost-benefit driver). For such a case, any dependency of the highly trustworthy component upon a less trustworthy component does not degrade the trustworthiness of the resulting low-trust system.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Relevant Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-8 (11)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles / Hierarchical Protection</td>
<td></td>
<td>implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].</td>
<td>The principle of hierarchical protection states that a component need not be protected from more trustworthy components, in the degenerate case of the most trustworthy component, it protects itself from all other components. For example, if an operating system kernel is deemed the most trustworthy component in a system, then it protects itself from all other components if it supports, but the applications, certainly, do not need to protect themselves from the kernel. The trustworthy components in a system is a consideration for applying the principle of hierarchical protection. A trusted system need not protect itself from an equally trustworthy user, reflecting use of untrusted systems in &quot;system high&quot; environments where users are highly trustworthy and where other protections are put in place to bound and protect the &quot;system high&quot; execution environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-8 (12)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles / Least Privilege</td>
<td></td>
<td>implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].</td>
<td>The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified function, but no more. Applying the principle of least privilege limits the scope of the component’s actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfacing used to create component capability are available to only certain subsets of the user population, and component designs support a sufficiently fine granularity of privilege limits the scope of the component’s actions, which has two desirable effects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally more costly to construct and implement, owing to increased types of development processes. Trusted components also require greater security analysis to satisfy their trustworthy states. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. Analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to assure than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-8 (13)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles / Minimized Security Elements</td>
<td></td>
<td>implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].</td>
<td>The principle of minimized security elements states that the system does not have dangerous untrusted components. The principle of minimized security elements has two aspects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally more costly to construct and implement, owing to increased types of development processes. Trusted components also require greater security analysis to satisfy their trustworthy states. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. The analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to assure than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-8 (14)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles / Threshold</td>
<td></td>
<td>implement the security design principle of threshold in [Assignment: organization-defined systems or system components].</td>
<td>The principle of threshold states that each system component is allocated sufficient privileges to accomplish its specified function, but no more. Applying the principle of least privilege limits the scope of the component’s actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfacing used to create component capability are available to only certain subsets of the user population, and component designs support a sufficiently fine granularity of privilege limits the scope of the component’s actions, which has two desirable effects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally more costly to construct and implement, owing to increased types of development processes. Trusted components also require greater security analysis to satisfy their trustworthy states. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. Analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to assure than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-5</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles / Least Privilege</td>
<td></td>
<td>implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].</td>
<td>The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified function, but no more. Applying the principle of least privilege limits the scope of the component’s actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfacing used to create component capability are available to only certain subsets of the user population, and component designs support a sufficiently fine granularity of privilege limits the scope of the component’s actions, which has two desirable effects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally more costly to construct and implement, owing to increased types of development processes. Trusted components also require greater security analysis to satisfy their trustworthy states. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. Analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to assure than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-6, CA-7</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles / Least Privilege</td>
<td></td>
<td>implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].</td>
<td>The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified function, but no more. Applying the principle of least privilege limits the scope of the component’s actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfacing used to create component capability are available to only certain subsets of the user population, and component designs support a sufficiently fine granularity of privilege limits the scope of the component’s actions, which has two desirable effects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally more costly to construct and implement, owing to increased types of development processes. Trusted components also require greater security analysis to satisfy their trustworthy states. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. Analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to assure than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-8</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles / Least Privilege</td>
<td></td>
<td>implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].</td>
<td>The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified function, but no more. Applying the principle of least privilege limits the scope of the component’s actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfacing used to create component capability are available to only certain subsets of the user population, and component designs support a sufficiently fine granularity of privilege limits the scope of the component’s actions, which has two desirable effects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally more costly to construct and implement, owing to increased types of development processes. Trusted components also require greater security analysis to satisfy their trustworthy states. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. Analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to assure than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-10</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles / Least Privilege</td>
<td></td>
<td>implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].</td>
<td>The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified function, but no more. Applying the principle of least privilege limits the scope of the component’s actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfacing used to create component capability are available to only certain subsets of the user population, and component designs support a sufficiently fine granularity of privilege limits the scope of the component’s actions, which has two desirable effects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally more costly to construct and implement, owing to increased types of development processes. Trusted components also require greater security analysis to satisfy their trustworthy states. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. Analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to assure than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].

The principle of secure distributed composition states that the composition of distributed components that enforce the same system security policy results in a system that enforces that policy at least as well as the individual components do. Many of the design principles for secure systems deal with how components can or should interact. The need to create or enable capability from the composition of distributed components can magnify the relevance of these principles. In particular, the translation of security policy from a centralized to a distributed system or a system-of-systems can have unexpected or emergent results. Communication protocols and distributed data consistency mechanisms help to ensure consistent policy enforcement across a distributed system. To ensure a system-wide level of assurance of correct policy enforcement, the security architecture of a distributed composite system is thoroughly analyzed.

Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].

The principle of trusted communications channels states that when communicating a system under reliance is a potential threat to communications between components (i.e., the interconnections between components), each communication channel is trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions). Trusted communication channels are achieved by a combination of restricting access to the communication channel (to ensure an acceptable match in the trustworthiness of the endpoints involved in the communication) and employing end-to-end protections for the data transmitted over the communication channel (to protect against interception, modification, and to further increase the assurance of proper end-to-end communications).

Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].

The principle of continuous protection states that components and data used to enforce the security policy have uninterrupted protection that is consistent with the security policy and the security architecture assumptions. No assurance that the system can provide the confidentiality, integrity, availability, and privacy protections for its design capability can be made if there are gaps in the protection. Any assurances about the ability to secure a relevant capability require that data and information are continuously protected. That is, there are no periods during which data and information are left unattended while under control of the system (i.e., during the transfer, storage, processing, or communication of the data and information, as well as during system initialization, execution, failure, interruptions, and shutdown). Continuous protection requires adherence to the principles of the reference monitor concept (i.e., every request is validated by the reference monitor, the reference monitor can protect itself from tampering, and sufficient assurance of the correctness and completeness of the mechanism can be ascertained from analysis and testing), and the principle of secure failure and recovery (i.e., preservation of a secure state during error, fault, failure, and successful attack; preservation of a secure state during recovery to normal, degraded, or alternate operational modes). Continuous protection also applies to systems designed to operate in varying circumstances, including those that deliver full operational capability and degraded-mode configurations that deliver partial operational capability. The continuous protection principle requires that changes to the system security policies be traceable to the operational event that drove the configuration and be verifiable (i.e., it is possible to verify that the proposed changes will not put the system into an insecure state). Insufficient traceability and verifiability may lead to inconsistent states or protection discontinuities due to the complex or undecidable nature of the problem. The use of pre-verified configuration definitions that reflect the new security policy enables analysis to determine that a transition from old to new policies is essentially secure, and that any residual effects from the old policy are guaranteed by not conflict with the new policy. The ability to demonstrate the apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. Metadata is bound to the target data that it describes in a way that the system can interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. The principle of secure metadata management states that metadata are "first class" objects with respect to security policy when the policy requires complete protection of information. It requires that the security subdomain be self-protecting. The principle of secure metadata management is achieved by the recognition that a system, subsystem, or component cannot achieve self-protection unless it protects the data it relies upon for correct execution. Data is generally not interpreted by the system that stores it. It may have semantic value (i.e., it carries information) to users and programs that process the data. In contrast, metadata is information about data, such as a file name or the date when the file was created. Metadata is bound to the target data that it describes in a way that the system can interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata. The apparent secondary nature of metadata can lead to a requirement for adequate traceability. Encryption is one of the security policies that includes the enforcement of information. A particular concern associated with insufficient protections for metadata is the ability of a system to interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the sensitivity level of a file name), to include self-referential metadata.
Implement the security design principle of self-analysis in (Assignment: organization-defined systems or system components). The principle of self-analysis states that a system component or user is able to assess its internal state and functionality in a measured state at various stages of execution, and that the self-analysis capability is communicated with the level of trustworthiness invested in the system. At the system level, a self-analysis can be achieved through hierarchical assessments of trustworthiness established in a bottom up fashion. In this approach, the lower level components check for data integrity and correct functionality by a limited subset of higher-level components. For example, trusted boot sequences involve a trusted lower-level component attesting to the trustworthiness of the next higher-level components so that a trusted chain of trust can be established. At the root, a component attests to itself, which usually involves an automatic or environment-enabled assumption about its integrity. Results of the self-analysis can be used to guard against externally induced errors, or internal malfunctions or transient errors. By following this principle, some simple errors or malfunctions can be detected without allowing the effects of the error or malfunction to propagate outside the component. Further, the self-test can also be used to assist in the configuration of the component, detecting any potential conflicts in configuration with respect to the expected configuration.

Implement the security design principle of accountability and traceability in (Assignment: organization-defined systems or system components). The principle of accountability and traceability states that it is possible to trace security-relevant actions (i.e., subject-agent interactions) in the entity, or subset thereof, the action is being taken. The principle of accountability and traceability requires a trustworthy infrastructure that can record details about actions that affect system security (e.g., on an audit sub-domain). To record the details about actions, the system is able to uniquely identify the entity or subset thereof the action is being carried out and also record the record of actions of sections that are carried out. The accountability policy also requires the audit trail of the generated access and modifications. The principle of trust should assist in tracing the actions in particular entities, as it increases the granularity of accountability. Accounting for actions with system/watermark, and ultimately with users, and making the audit trail secure against unauthorized access and modifications provides non-repudiation, because once an action is recorded, it is not possible to change the audit trail. Another important function that accountability and traceability serve is in the routine and forensic analysis of events associated with the violation of security policy. Analysis of audit logs may provide additional information that may be helpful in determining the path or component that allowed the violation of the security policy, and the actions of individuals associated with the violation of security policy.

Implement the security design principle of secure defaults in (Assignment: organization-defined systems or system components). The principle of secure defaults states that the default configuration of a system should include a default security configuration by which a service, systems, or system components can be configured to meet the security level expected by the organization or user. The principle of secure defaults also applies to the initial i.e., default configuration of a system as well as to the security engineering and design of access control and other security functions. The principle of secure defaults states that secure defaults should be a part of the system so that the actions of the system can be allowed that the actions of the attacker are not allowed. A system should be designed such that the actions of the attacker are not allowed. When a system is designed, the actions of the attacker are not allowed. A system should be designed such that the actions of the attacker are not allowed. When a system is designed, the actions of the attacker are not allowed. A system should be designed such that the actions of the attacker are not allowed. When a system is designed, the actions of the attacker are not allowed. A system should be designed such that the actions of the attacker are not allowed. When a system is designed, the actions of the attacker are not allowed. A system should be designed such that the actions of the attacker are not allowed. When a system is designed, the actions of the attacker are not allowed.

Financial management involves the ability to balance the requirement of the system to ensure that security policies are not violated. The regularity of enforcement to ensure that the system is capable of detecting breaches of system and recording breaches at the same time. By following this principle, the system is able to uniquely identify the entity, or subset thereof, the action is being taken. The principle of accountability and traceability requires an audit trail that is secure against unauthorized access and modifications. The principle of trust should assist in tracing the actions in particular entities, as it increases the granularity of accountability. Accounting for actions with system/watermark, and ultimately with users, and making the audit trail secure against unauthorized access and modifications provides non-repudiation, because once an action is recorded, it is not possible to change the audit trail. Another important function that accountability and traceability serve is in the routine and forensic analysis of events associated with the violation of security policy. Analysis of audit logs may provide additional information that may be helpful in determining the path or component that allowed the violation of the security policy, and the actions of individuals associated with the violation of security policy.

Implement the security design principle of secure failure and recovery in (Assignment: organization-defined systems or system components). The principle of secure failure and recovery states that neither a failure in a system function or mechanism nor any recovery strategy that parallel this principle to provide the ability to detect and recover from failure. The security engineering approach to this principle states that security mechanisms deny requests unless the request is found to be well formed and consistent with the security policy. The secure alternative is to follow a request in which it is determined that the request is well-formed and consistent with the policy. In a larger system, the conditions that are satisfied to grant a request that is a step-defined are often for more complex and complete than those that would need to be checked in order to deny a request that is not defined granted.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-8 (25)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td></td>
<td>Implement the security design principle of human factored security in (Assignment: organization-defined systems or system components).</td>
<td>The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions. The device that effect such policy and enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also use an interface that is meaningful, clear, and relevant feedback and warnings when necessary. The security mechanisms are designed to be intuitive, user-friendly, and provide feedback for user actions. The personnel with system administrative and operation responsibilities are able to configure systems before start-up and administer them during runtime, in both cases with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impair or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the resources necessitated for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable or avoid them, or use the mechanisms in ways inconsistent with the security requirements and protection needs the mechanisms were designed to satisfy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-8 (26)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td></td>
<td>Implement the security design principle of human factored security in (Assignment: organization-defined systems or system components).</td>
<td>The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions. The device that effect such policy and enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also use an interface that is meaningful, clear, and relevant feedback and warnings when necessary. The security mechanisms are designed to be intuitive, user-friendly, and provide feedback for user actions. The personnel with system administrative and operation responsibilities are able to configure systems before start-up and administer them during runtime, in both cases with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impair or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the resources necessitated for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable or avoid them, or use the mechanisms in ways inconsistent with the security requirements and protection needs the mechanisms were designed to satisfy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-10 (21)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td></td>
<td>Implement the security design principle of human factored security in (Assignment: organization-defined systems or system components).</td>
<td>The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions. The device that effect such policy and enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also use an interface that is meaningful, clear, and relevant feedback and warnings when necessary. The security mechanisms are designed to be intuitive, user-friendly, and provide feedback for user actions. The personnel with system administrative and operation responsibilities are able to configure systems before start-up and administer them during runtime, in both cases with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impair or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the resources necessitated for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable or avoid them, or use the mechanisms in ways inconsistent with the security requirements and protection needs the mechanisms were designed to satisfy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-1 (27)</td>
<td>2</td>
<td>System and Services Acquisition / Security and Privacy Engineering Principles</td>
<td></td>
<td>Implement the security design principle of human factored security in (Assignment: organization-defined systems or system components).</td>
<td>The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions. The device that effect such policy and enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also use an interface that is meaningful, clear, and relevant feedback and warnings when necessary. The security mechanisms are designed to be intuitive, user-friendly, and provide feedback for user actions. The personnel with system administrative and operation responsibilities are able to configure systems before start-up and administer them during runtime, in both cases with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impair or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the resources necessitated for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable or avoid them, or use the mechanisms in ways inconsistent with the security requirements and protection needs the mechanisms were designed to satisfy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM-1</td>
<td></td>
<td></td>
<td></td>
<td>Implement the security design principle of human factored security in (Assignment: organization-defined systems or system components).</td>
<td>The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions. The device that effect such policy and enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also use an interface that is meaningful, clear, and relevant feedback and warnings when necessary. The security mechanisms are designed to be intuitive, user-friendly, and provide feedback for user actions. The personnel with system administrative and operation responsibilities are able to configure systems before start-up and administer them during runtime, in both cases with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impair or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the resources necessitated for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable or avoid them, or use the mechanisms in ways inconsistent with the security requirements and protection needs the mechanisms were designed to satisfy.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SA-9 (1) 2  System and Services Acquisition | Security and Privacy Engineering Principles | Procedural Rigor
Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].

The principle of procedural rigor states that the rigor of a system life cycle process is commensurate with its intended trustworthiness. Procedural rigor defines the scope, depth, and detail of the system life cycle procedures. Rigorous system life cycle procedures contribute to the assurance that the system is correct and free of unintended functionality in several ways. First, the procedures impose checks and balances on the life cycle process such that the introduction of unexpected functionality is prevented. Second, rigorous procedures applied to systems security engineering activities that produce specifications and other system design documents contribute to the ability to understand the system or its design, rather than trusting that the component is implemented as the authoritative (and potentially misleading) specification. Finally, modifications to an existing system component are easier when there are defined specifications describing its current design, instead of studying source code or schematics to try to understand how it works. Procedural rigor helps to ensure that security functions and assurance requirements have been satisfied, and it contributes to a better-informed basis for the determination of trustworthiness and risk posture. Procedural rigor is communicated with the degree of assurance desired for the system. If the required trustworthiness of the system is low, a high level of procedural rigor may add unnecessary cost, whereas when high trustworthiness is critical, the cost of high procedural rigor is justified.

SA-8 (2) 2  System and Services Acquisition | Security and Privacy Engineering Principles | Secure System Modification
Implement the security design principle of sufficient documentation in [Assignment: organization-defined systems or system components].

The principle of sufficient documentation states that system documentation maintains system security with respect to the security requirements and risk tolerance of stakeholders. Sufficient documentation in systems and systems transforms systems into systems that are not secure. The procedures for system modification ensure that, if the system is in violation of the requirements, the system that was applied to its initial development is applied to any system change. Because modifications can affect the ability of the system to maintain its secure state, a careful security analysis of the modification is needed prior to its implementation and deployment. This principle provides the principle of secure modularity.

SA-9 (1) 1  System and Services Acquisition | External System Services
(a) Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls].
(b) Define and document organizational oversight and user roles and responsibilities with regard to external system services; and
(c) Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].

External system services are services that are provided by an external provider and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, subcontracts, and agreements. The responsibility for managing these systems, including those under the control of an organization, remains with the organization. Systems or system components outside the control of organizations must be managed in accordance with the organization's risk level. The control system components can be shared with the organization for purposes of protecting the services provided by the organization.

SA-8 (3) 2  System and Services Acquisition | External System Services | Risk Assessments and Organizational Approaches
Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services, and
(a) verify that the acquisition or outsourcing of information security services is approved by [Assignment: organization-defined personnel or roles].

Information security services include the operation of security devices such as firewalls, firewalls and firewalls, and incident monitoring, analysis, and response. Risk assessment can include system, mission or business, privacy, or supply chain risks.

SA-9 (1) 2  System and Services Acquisition | External System Services | Establish and Maintain Trust Relationship with Providers
Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].

The degree of confidence that the external service is an acceptable external service provider is a function of the trust that organizations place in the external provider, individually or in combination. Trust relationships can help organizations to gain increased levels of confidence that participating service providers are providing adequate protection for the service rendered and can also be used when conducting incident response or when planning for upgrades or obsolescence. Trust relationships can be complacency due to the potentially large number of entities participating in the consumer-provider interactions, relationships between and levels of trust, and types of interactions between the parties. In some cases, the degree of trust is based on the level of control organizations can exert on external service providers regarding the controls necessary for the protection of the service, information, or individual privacy and the evidence brought forth as to the effectiveness of the implemented controls. The level of control is established by the terms and conditions of the contracts or service-level agreements.
SA-9 (8) 2 System and Services Acquisition / External System Services | External System

Restrict the geographic location of information processing and data storage to facilities located within the legal jurisdictional boundary of the United States.

The geographic location of information processing and data storage can have a direct impact on the ability of organizations to successfully execute their core mission and business functions. High impact information and systems, if compromised or breached, can have a severe or catastrophic adverse impact on organizational assets and operations, individuals, other organizations, and the Nation. Restricting the processing and storage of high impact information to facilities within the legal jurisdictional boundary of the United States provides greater control over such processing and storage.

SA-10 1 System and Services Acquisition / Developer Configuration Management

require the developer of the system, system component, or system service to:
- a. Perform configuration management during system, component, or service [selection (or more) design, development, implementation, operation, disposal];
- b. Document, manage, and control the integrity of changes to [assignment: organization-defined configuration items under configuration management];
- c. Implement only organization-approved changes to the system, component, or service;
- d. Discern approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
- e. Track security flaws and flaw resolution within the system, component, or service and report findings to [assignment: organization-defined personnel].

Organizations consider the quality and completeness of configuration management practices conducted by developers as direct evidence of applying effective security controls. Controls include protecting from unauthorized modification or destruction, the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the system, component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes. The configuration items that developers and configuration management processes include: formal model, the functional, high level, and low level design specifications, other design data, implementation documentation, source code and hardware schematics, the current running version of the object code, tools for comparing new versions of security relevant hardware descriptions and source code with previous versions, and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

SA-11 (2) 2 System and Services Acquisition / Developer Configuration Management / Software and Firmware Integrity Verification

require the developer of the system, component, or system service to enable integrity verification of software and firmware components.

Software and firmware integrity verification allows organizations to detect unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms. The integrity checking mechanism can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.

SA-11 (2) 2 System and Services Acquisition / Developer Configuration Management / Alternative Configuration Management

provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

Alternative configuration management processes may be required, for example, when configuration management of off-the-shelf information technology products. Alternate configuration management processes include organizational personnel that review and propose proposed changes to systems, system components, and system services, and that conduct security and privacy impact analyses prior to the implementation of changes to systems, components, or services.

SA-11 (2) 2 System and Services Acquisition / Developer Configuration Management / Hardware Integrity Verification

require the developer of the system, component, or system service to enable integrity verification of hardware components.

Hardware integrity verification allows organizations to detect unauthorized changes to hardware components using developer-provided tools, techniques, methods, and mechanisms. Organizations verify the integrity of hardware components, for example, with tamper-proof labels and serial number records provided by developers and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include hardware and firmware updates to such components.

SA-11 (2) 2 System and Services Acquisition / Trusted Generation

require the developer of the system, component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.

Trusted generation of descriptions, source code, and object code addresses unauthorized changes to hardware, software, and firmware components between versions during development. The focus is on the efficacy of the configuration management process by the developer to ensure that newly generated versions of security-relevant hardware descriptions, source code, and object code continue to enforce the security policy for the system, system component, or system service. In contrast, SA-10(1) and SA-10(2) allow organizations to detect unauthorized changes to hardware, software, and firmware components using tools, techniques, or mechanisms provided by developers.
SA-11 1 System and Services Acquisition | Developer Testing and Evaluation

Require the developer of the system, system component, or system service to perform penetration testing:

(a) Uses the following contextual information: [Assignment: organization-defined information concerning the system, system component, or service that:

i. Defines and explains a test plan for ongoing security and privacy assessments; ii. Perform [Selection (one or more): unit, unit integration, system, regression] testing/evaluation [Assignment: organization-defined frequency] of [Assignment: organization-defined depth and coverage]; iii. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; and iv. Implement a verifiable flow remediation process; and

v. Correct flaws identified during testing and evaluation.

b. For the current version.

c. Specify the acceptance criteria for security and privacy assessment plans, flaw remediation requirements for documentation.

The trusted distribution of security-relevant hardware, software, and firmware updates helps to ensure that the updates are correct representations of the master copies transmitted by the developer and have not been tampered with during distribution.

SA-11 2 System and Services Acquisition | Developer Testing and Evaluation | Static Code Analysis

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code and checking for incorporation of libraries or other included code with known vulnerabilities or that are out of date and not supported. Static code analysis can also be used to identify vulnerabilities and to enforce secure coding practices and static code analysis is most effective when used early in the development process, where each code change can be systematically scanned for potential security weaknesses. Static code analysis can provide clear remediation guidance along with advice to enable developers to fix such defects. Evidence of current implementation of static analysis include aggregate defect severity for critical defect types; evidence that defects were inspected by developers or security professionals; and evidence that defects were remediates. A high density of open bugs, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

SA-11 2 System and Services Acquisition | Developer Testing and Evaluation | Threat Modeling and Indiciability Analysis

Require the developer of the system, system component, or system service to perform threat modeling and indiciability analysis during development and the subsequent testing and evaluation of the system, component, or service that:

(a) Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, desired or assumed threats, and acceptable risk levels];

(b) Uses the following tools and methods: [Assignment: organization-defined tools and methods];

(c) Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and

(d) Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].

SA-11 2 System and Services Acquisition | Developer Testing and Evaluation | Penetration Testing

Require the developer of the system, system component, or system service to perform penetration testing:

(a) At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; and

(b) Using the following constraints: [Assignment: organization-defined constraints].

Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent implemented security and privacy features of information technology products and systems. Information for assessors conducting penetration testing includes product and system design specifications, source code, and administrative and operator manuals. Penetration testing can include white-box, gray-box, or black-box testing with analysts performed by skilled professionals simulating adversary actions. The objective of penetration testing is to discover vulnerabilities in systems, system components, and services resulting from information entry, configuration faults, or other operational weaknesses or deficiencies. Penetration testing can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible. Where user sensitive information and other personally identifiable information is captured or recorded during penetration testing, such information is handled appropriately to protect privacy.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA-12 (5)</td>
<td>2</td>
<td>System and Services Acquisition / Developer Testing and Evaluation / Attack Surface Reviews</td>
<td>X</td>
<td>Require the developer of the system, system component, or system service to perform attack surface reviews. Attack surfaces of systems and system components are exposed areas that make those systems more vulnerable to attacks. Attack surfaces include any accessible areas where weaknesses or defects in the hardware, software, and firmware components provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers analyze the design and implementation changes to systems and mitigate attack surfaces generated as a result of the changes. Correction of identified flaws includes deprecation of unsafe functions.</td>
<td></td>
<td>SA-13</td>
<td></td>
</tr>
<tr>
<td>SA-11 (2)</td>
<td>2</td>
<td>System and Services Acquisition / Developer Testing and Evaluation / Verify Source of Testing and Evaluation</td>
<td></td>
<td>Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: Assignment: organization-defined breadth and depth of testing and evaluation.</td>
<td>Verify that testing and evaluation provides complete coverage of required controls can be accomplished by a variety of analytical techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Reasonable formal testing coverage at the highest level of assurance can be provided using formal modeling and analysis techniques, including simulation between control implementation and corresponding test cases.</td>
<td>SA-13</td>
<td></td>
</tr>
<tr>
<td>SA-11 (4)</td>
<td>2</td>
<td>System and Services Acquisition / Developer Testing and Evaluation / Dynamic Code Analysis</td>
<td></td>
<td>Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis. Systematic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to ensure that security functionality performs in the way it was designed. A specialized type of dynamic analysis, known as fuzz testing, involves program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the associated functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines called during execution of the test suite) and code concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).</td>
<td>Interactive (also known as instrumentation-based) application security testing is a method of detecting vulnerabilities by analyzing applications as they run during testing. The use of instrumentation means direct measurements of the actual runtime applications, and uses access to the code, user interface, libraries, frameworks, backend connections, and codebases to measure control effectiveness directly. When combined with analysis techniques, interactive application security testing can identify a broad range of potential vulnerabilities and snoop control effectiveness. Instrumentation-based testing works in real time and can be used continuously throughout the system development life cycle.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-12 (1)</td>
<td>1</td>
<td>System and Services Acquisition / Supply Chain Protection</td>
<td>X</td>
<td>(Withdrawn: Moved to SA-20)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Acquisition Strategies / Tools / Methods</td>
<td>X</td>
<td>(Withdrawn: Incorporated into RA-9)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Supplier Reviews</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Thwarting Phishing and Whaling</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-5)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Diversity of Suppliers</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Limitation of Access</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Minimizing Recruitment Tame</td>
<td>X</td>
<td>(Withdrawn: Incorporated into SA-8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Assessments Prior to Selection / Insurance Program</td>
<td>X</td>
<td>(Withdrawn: Incorporated into SA-8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Surveillance Security</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-5)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Avoiding as Genuine and Not Alarmed</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Avoiding as Anomalous and Suspicious</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Forensic Testing / Analysis of Attribution Processes and Actions</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Inter-organizational Agreements</td>
<td>X</td>
<td>(Withdrawn: Incorporated into MA-6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Critical Information System Components</td>
<td>X</td>
<td>(Withdrawn: Incorporated into MA-6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Identity and Traceability</td>
<td>X</td>
<td>(Withdrawn: Moved to SR-5)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Processes to Avoid Concentration or Over-reliance</td>
<td>X</td>
<td>(Withdrawn: Incorporated into MA-6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA-11 (1)</td>
<td>2</td>
<td>System and Services Acquisition / Supply Chain Protection / Critical Components with No Viable Alternative</td>
<td>X</td>
<td>(Withdrawn: Incorporated into SA-20)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SA-15 (2) 2 System and Services Acquisition | Development Process, Standards, and Tools | Security Training Task

Require the developer of the system, system component, or system service to select and employ security and privacy training tools for use during the development process.

- Development training tools select and deploy security and privacy tracking tools, including vulnerability or work done tracking systems that facilitate assignment, tracking, polling, and tracking of completed work items or tasks associated with development processes.

SA-15 (2) 3 System and Services Acquisition | Development Process, Standards, and Tools | Security Training Task

Require the developer of the system, system component, or system service to select and employ security and privacy training tools, including vulnerability or work done tracking systems that facilitate assignment, tracking, polling, and tracking of completed work items or tasks associated with development processes.

SA-15 (2) 4 System and Services Acquisition | Development Process, Standards, and Tools | Security Training Task

Require the developer of the system, system component, or system service to select and employ security and privacy training tools, including vulnerability or work done tracking systems that facilitate assignment, tracking, polling, and tracking of completed work items or tasks associated with development processes.

SA-15 (3) 1 System and Services Acquisition | Development Process, Standards, and Tools

1. Require the developer of the system, system component, or system service to follow a documented development process that:
   - (a) Equally addresses security and privacy requirements; and
   - (b) Identifies the standards and tools used in the development process;
   - (c) Documents the specific tools and tool configurations used in the development process; and
   - (d) Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
   - (e) Reviews the development process, standards, tools, tool options, and tool configurations (Assignment: organization-defined frequency) to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: (Assignment: organization-defined security and privacy requirements).

Discussion: Development tools include programming languages and computer-aided design systems. Review of development processes include the use of maturity models to determine the potential effectiveness of such processes; maintaining the integrity of changes to tools and tools facilitates effective supply chain risk assessment and mitigation. In particular, such requirements include configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes.


Require the developer of the system, system component, or system service to ensure the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: (Assignment: organization-defined training).

- The incident response plan provided by developers may be incorporated into organizational incident response plans. Developer incident response plans provide information that is not readily available to organizations. Such information may be extremely helpful, for example, when organizations respond to vulnerabilities in commercial off-the-shelf products.


Require the developer of the system, system component, or system service to ensure the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: (Assignment: organization-defined training).

- Requirements on systems or system components may exist within developer organizations. Vulnerability information is available from a variety of public and private sources, including the National Vulnerability Database.


Require the developer of the system, system component, or system service to ensure the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: (Assignment: organization-defined training).

- Criticality analysis performed by the developer provides input to the criticality analysis performed by organizations. Developer input is essential to organizational criticality analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes functional specifications, high-level designs, low-level designs, and source code and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. High value assets can be moderate- or high-impact systems due to heightened adversarial interest or potential adverse effects on the federal enterprise. Developer input is especially important when organizations conduct supply chain criticality analyses.
SA-17 (1) 2 System and Services Acquisition | Developer Security Architecture and Design

Require the developer of the system, system component, or system service to:

(a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware; and
(b) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(c) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification that are strictly internal to the security-relevant hardware, software, and firmware.

Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details that are present have no impact on the behaviors or policies being modeled. Formal methods can be useful to show that the high-level security properties are satisfied by the formal system description, and that the formal system description is correctly implemented by a description of some lower level, including a hardware description. Consistency between the formal top-level specification and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to demonstrate such consistency. Consistency between the formal top-level specification and the actual implementation may require the use of an informal demonstration due to limitations in the applicability of formal methods to prove that the specification accurately reflects the system, component, or service that is trusted to perform correctly to maintain required security properties.

Correspondence is also less prone to error (see AC-25, SA-8, SC-3).

SA-17 (2) 2 System and Services Acquisition | Developer Security Architecture and Design | Security-relevant Components

Require the developer of the system, system component, or system service to:

(a) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete;
(b) Show that the definition for security-relevant hardware, software, and firmware is complete;
(c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(d) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(e) Show via informal demonstration, that the formal policy model completely covers the interfaces to security-relevant hardware, software, and firmware; and
(f) Show via informal demonstration, that the formal policy model completely covers the interfaces to security-relevant hardware, software, and firmware; and
(g) Show via informal demonstration, that the formal policy model is consistent with the formal policy model.

Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details that are present have no impact on the behaviors or policies being modeled. Formal methods can be useful to show that the high-level security properties are satisfied by the formal system description, and that the formal system description is correctly implemented by a description of some lower level, including a hardware description. Consistency between the formal top-level specification and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to demonstrate such consistency. Consistency between the formal top-level specification and the actual implementation may require the use of an informal demonstration due to limitations in the applicability of formal methods to prove that the specification accurately reflects the system, component, or service that is trusted to perform correctly to maintain required security properties.

Correspondence is also less prone to error (see AC-25, SA-8, SC-3).

SA-17 (3) 2 System and Services Acquisition | Developer Security Architecture and Design | Informal Correspondence

Require the developer of the system, system component, or system service to:

(a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;
(b) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(d) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(e) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(f) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(g) Show via informal demonstration, that the descriptive top-level specification is consistent with the formal policy model.

Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details that are present have no impact on the behaviors or policies being modeled. Formal methods can be useful to show that the high-level security properties are satisfied by the formal system description, and that the formal system description is correctly implemented by a description of some lower level, including a hardware description. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to demonstrate such consistency. Hardware, software, and firmware mechanisms internal to security-relevant hardware, software, and firmware include mapping regions and direct memory input and output.

Correspondence is also less prone to error (see AC-25, SA-8, SC-3).

SA-17 (4) 2 System and Services Acquisition | Developer Security Architecture and Design | Conceptually Simple Design

Require the developer of the system, system component, or system service to:

(a) Produce, as an integral part of the development process, a conceptual simple design specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;
(b) Show via informal demonstration, that the conceptual simple design specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(c) Show via informal demonstration, that the conceptual simple design specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(d) Show via informal demonstration, that the conceptual simple design specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(e) Show via informal demonstration, that the conceptual simple design specification completely covers the interfaces to security-relevant hardware, software, and firmware; and
(f) Show via informal demonstration, that the conceptual simple design specification is consistent with the formal policy model.

Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details that are present have no impact on the behaviors or policies being modeled. Formal methods can be useful to show that the high-level security properties are satisfied by the formal system description, and that the formal system description is correctly implemented by a description of some lower level, including a hardware description. Consistency between the conceptual simple design specification and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to demonstrate such consistency. Hardware, software, and firmware mechanisms internal to security-relevant hardware, software, and firmware include mapping regions and direct memory input and output.

Correspondence is also less prone to error (see AC-25, SA-8, SC-3).

SA-17 (5) 2 System and Services Acquisition | Developer Security Architecture and Design | Structure for Testing

Require the developer of the system, system component, or system service to:

(a) Produce, as an integral part of the development process, a structure for testing description that specifies the interfaces to security-relevant hardware, software, and firmware to facilitate testing.

Applying the security design principles in [SP 800-160 v1] promotes complete, consistent, and comprehensive testing and evaluation of systems, system components, and services. The thoroughness of such testing contributes to the evidence produced to generate an effective assurance case or argument as to the trustworthy nature of the system, system component, or service.
The principle of least privilege states that each component is allocated sufficient privileges to accomplish its specified functions, but no more (see SA-8(14)). Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects: first, the security impact of a failure, corruption, or misuse of the system component results in a minimized security impact. Second, the security analysis of the component is simplified. Least privilege is a pervasive principle that is reflected in all aspects of the system security design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports it effectively (e.g., privileging of active components is managed with an interface for the audit manager, who ensures that audit data is collected and stored; and, finally, an interface for the audit reviewer, who has read only access to view the audit data). Organizations that have already built systems but need to perform operations on them often need to add security mechanisms, and least privilege can be used as a guiding principle for the internal structure of the system itself. Our approach to least privilege is to construct modules so that the only elements exposed to the module are directly operational upon the function within the module. Elements external to a module that may be affected by the module’s operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements. Another aspect of least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality, and that the access modes to the elements (e.g., read, write) are minimal.

Restrained Controls

Page 82 of 108
a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
b. Provide the following options for alternative sources for continued support for unsupported components: (Selection one or more): in-house support, (Assignment: organization-defined support from external provider).

Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components, for example, when vendors no longer provide critical software patches or product updates, provide an opportunity for vulnerabilities to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturer, developers, or vendors when such components are essential to organizational mission and business operations. If necessary, organizations can establish in-house support by developing customized patches for critical software components or alternatively, obtain the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include Open Source Software value-added vendors.

SA-22 1 System and Services Acquisition | Unsupported System Components

Employ (Selection one or more): design modification; augmentation; reconfiguration on (Assignment: organization-defined systems or system components) supporting mission essential services or functions to increase the trustworthiness in those systems or components.

It is often necessary for a system or system component that supports mission essential services or functions to be enhanced to maintain the trustworthiness of the resources. Sometimes this enhancement is done at the design level. In other instances, it is done post-design, either through modifications of the system in question or by augmenting the system with additional components. For example, supplemental authentication or non-repudiation functions may be added to the system to enhance the identity of critical resources to other resources that depend upon the organization-defined resources.

SA-23 1 System and Services Acquisition | Specialization

Prevent the presentation of system management functionality at interfaces to non-privileged users. Preventing the presentation of system management functionality at interfaces to non-privileged users involves isolating system management functional and the user interface and does so in two general ways: by preventing the presentation of any system management functionality from an interface to any user, or separating user functionality from system management functionality. System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations implement separation of system management functions from user functions, for example, by using different computers, instances of operating systems, central processing units, or network addresses, by employing virtualization techniques, or some combination of these or other methods. Separation of system management functions from user functions includes online administrative interfaces that separate administrative user interface from other user interface.

It is often necessary for a system or system component that supports mission essential services or functions to be enhanced to maintain the trustworthiness of the resources. Sometimes this enhancement is done at the design level. In other instances, it is done post-design, either through modifications of the system in question or by augmenting the system with additional components. For example, supplemental authentication or non-repudiation functions may be added to the system to enhance the identity of critical resources to other resources that depend upon the organization-defined resources.

For the benefits of allowing system management functionality to be presented at user interfaces, organizations typically require that the interface be protected through authentication and authorization. These security mechanisms ensure that only users with the appropriate privileges and permissions are allowed access to system management functionality.

This control addresses policy and procedures for the control in the SC family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may dictate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Resisting controls does not constitute an organizational policy or procedure.

AC-4, AC-6, SC-1, SC-7, SC-12, SC-15, SC-18

This control addresses policy and procedures for the control in the SC family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may dictate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Resisting controls does not constitute an organizational policy or procedure.

AC-3

This control addresses policy and procedures for the control in the SC family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may dictate the need for system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Resisting controls does not constitute an organizational policy or procedure.

AC-5
SC-3 (1) 2 System and Communications Protection | Security Function Isolation | Access and Role Control Functions

Restrict the ability of individuals to launch the following denial of service attacks against other systems: [Assignment: organization-defined denial of service attacks].

Restrict the ability of individuals to launch denial of service attacks against the mechanisms commonly used for such attacks are unobservable. Individuals of concern include hostile insiders or external adversaries that have breached or compromised the system and are using the system to launch a denial of service attack. Organizations can restrict the ability of individuals to connect to and remain online by terminating communication protocols (e.g., Telnet, HTTP). A variety of technologies are available to limit or eliminate the origination and effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect system components from being directly affected by, or the source of, denial of service attacks. Deploying increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial of service events.

SC-4 (1) 2 System and Communications Protection | Information in Shared System Resources | Security Levels

Information stored in shared system resources that can directly impact the security functions of systems. The fundamental design objective is to secure the specific portions of systems providing information security of minimal size and complexity. Minimizing the number of security functions in the security-relevant system components allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By restricting the security functions within the isolation boundaries, the amount of code that is required to enforce security policies is significantly reduced, thus contributing to understandability.

SC-4 (1) 2 System and Communications Protection | Security Function Isolation | Module Coupling and Cohesion

Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

The detection in the tiered module interaction helps to contain security functions and manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on others. Cohesion refers to the relationship between functions within a module. Better practices in software engineering and systems security engineering rely on layering, minimization, and module decomposition to reduce and manage complexity. This produces software modules that are highly cohesive and loosely coupled.

SC-4 (1) 2 System and Communications Protection | Information in Shared System Resources | Security Levels

Prevent unauthorized and unintended information transfer via shared system resources.

Changes in processing levels during system operation can occur, for example, during multithreaded or periodic processing with information of different classification levels or security categories. It can also occur during normal use of hardware components at different classification levels. Organizations can implement procedures to ensure secure information flows.

SC-6 1 System and Communications Protection | Resource Availability

Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection: one or more] priority quotas, [Assignment: organization-defined controls].

Priority protection prevents lower-priority processes from disturbing or interfering with the system servicing higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to system components for which there are only single users or roles.
(b) Audit the identity of internal users associated with denied communications. [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].

Deny network communications traffic by default and allow network communications traffic by exception where appropriate.

(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

(f) Prevent unauthorized exchange of control plane traffic with external networks; and

(e) Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need; and

(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need; and

(c) Protect the confidentiality and integrity of the information being transmitted across each interface; and

(b) Implement a managed interface for each external telecommunication service; and

(a) Implement a managed interface for each external telecommunication service; and

Limit the number of external network connections to the system. Limiting the number of external network connections facilitates monitoring of inbound and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Internal threats to external systems include threats to the security of external systems. Examples of control plane traffic include routing, domain name system (DNS), and management. Unauthorized control plane traffic can occur for example, through a technique known as "spoofing."

Denying by default and allowing by exception applies to both internal and external network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and agendum are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

Limit the number of external network connections to the system. Limiting the number of external network connections facilitates monitoring of inbound and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Internal threats to external systems include threats to the security of external systems. Examples of control plane traffic include routing, domain name system (DNS), and management. Unauthorized control plane traffic can occur for example, through a technique known as "spoofing."

Detecting outgoing communications traffic from internal systems that may pose threats to external networks is known as extrusion detection. Extrusion detection is carried out at managed interfaces (e.g., routing to an external service such as a remote devices. Prevent a remote device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Prevention of split tunneling is implemented in remote devices through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being configurable by users. Prevention of split tunneling is implemented within the system by the detection of split tunneling (i.e., configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and theft of organizational information.

External commercial telecommunications services may provide access to or allow communications services. Examples of control plane traffic include routing, domain name system (DNS), and management. Unauthorized control plane traffic can occur for example, through a technique known as "spoofing."

Split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and theft of organizational information.

External commercial telecommunications services may provide access to or allow communications services. Examples of control plane traffic include routing, domain name system (DNS), and management. Unauthorized control plane traffic can occur for example, through a technique known as "spoofing."

Managed interfaces include gateways, routers, firewalls, guard devices, and network-based intrusion detection and prevention systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). Preventing or prohibiting incoming or outgoing communications traffic within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. Common communication services are provided by network components and consolidated management systems shared by customers. These services may also include third party provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions.
Protection | Dynamic Isolation and Segregation

Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].

Several source address validation techniques should be applied to restrict the use of illegal and unauthorized source addresses and source addresses that should not be used inside the system boundary. Restrictions of incoming communications traffic provides determinations that source and destination address pairs which represent authorized or allowed communications. Determinations can be based on several factors, including the presence of such address pairs in the list of authorized or allowed communications; the absence of such address pairs in lists of unauthorized or disallowed pairs; or meeting some generic rule for authorized or allowed source and destination pairs. String authentication of network addresses is not possible without the use of explicit security protocols and thus, addresses can often be spoofed. Further, identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.

Protection | Prevent Discovery of Components and Devices

Protect the discovery of specific system components that represent a managed interface. This control enhancement protects network addresses of system components that are part of managed interfaces from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery, requiring prior knowledge for access. Preventing discovery of components and devices can be accomplished by not publishing network addresses, using network address translation, or not entering the addresses in domain name systems. Another prevention technique is to periodically change network addresses.

Protection | Prevent Discovery of Components and Devices

Protect systems from entering unsecured states in the event of an operational failure of a boundary protection device. The access is to conditions achieved by implementing mechanisms to ensure that in the event of operational failures of boundary protection devices [Assignment: organization-defined managed interfaces] requires that firewalls, and XML gateways. The devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layer.

Protection | Fail Secure

Block inbound and outbound communications traffic between [Assignment: organization-defined communication client] that are independently configured by end users and external service providers. Communication clients independently configured by end users and external service providers include instant messaging clients. Traffic blocking does not apply to communication clients that are configured by an organization to perform authorized functions.

Protection | Dynamic Isolation and Segregation

Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components. This is necessary to partition or separate system components of questionable origins from those components assessing greater trustworthy. Component isolation reduces the attack surface of organizational systems. Isolating selected system components can also limit the damage from successful attacks when such attacks occur.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC-7 (21)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Separate Subnets for Connecting to Different Security Domains</td>
<td></td>
<td>Implement separate network addresses to connect to systems in different security domains.</td>
<td>The decommissioning of systems into subnets (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains containing information with different security categories or classification levels.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-7 (22)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Implement Separate Feedback on Protocol Validation Failure</td>
<td></td>
<td>Disable feedback to systems on protocol validation failure.</td>
<td>Disabling feedback to systems when there is a failure in protocol validation prevents information from exfiltration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-7 (23)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Prevent Identity Theft</td>
<td></td>
<td>Prevent identity theft that would otherwise be untraceable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-7 (24)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Prevent Identity Theft</td>
<td></td>
<td>Prevent the processing of personally identifiable information.</td>
<td>Managing the processing of personally identifiable information is an important aspect of preventing an individual’s privacy. Applying, monitoring, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-7 (25)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Unrestricted National Security System Connections</td>
<td></td>
<td>Prevent the direct connection of an unclassified national security system to an external network without the use of an assignment (assignment-defined boundary protection device).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-7 (26)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Unrestricted National Security System Connections</td>
<td></td>
<td>Prevent the direct connection of a classified national security system to an external network without the use of an assignment (assignment-defined boundary protection device).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-7 (27)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Unrestricted National Security System Connections</td>
<td></td>
<td>Prevent the direct connection of an assignment-defined non-national security system to an external network without the use of an assignment (assignment-defined boundary protection device).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-7 (28)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Connections to Public Networks</td>
<td></td>
<td>Prevent the direct connection of an assignment-defined system to a public network.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-7 (29)</td>
<td>2</td>
<td>System and Communications Protection / Boundary Protection / Separate Subject to Identifier Functions</td>
<td></td>
<td>Implement (selection): physically, logically separate subnets to isolate the following system components and functions; (assignment): organization-defined critical system components and functions.</td>
<td>Balancing critical system components and functions from other noncritical system components and functions through separate subnets may be necessary to reduce the susceptibility to a catastrophe or a malicious breach or compromise resulting in system failure. For example, physically separating the command and control function from the assurance function through separate subnets in a commercial aircraft provides an increased level of assurance in the transactions of critical system functions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-8</td>
<td>1</td>
<td>System and Communications Protection / Transmission Confidentiality and Integrity</td>
<td></td>
<td>Protect the (selection [one or more]: confidentiality, integrity) of transmitted information.</td>
<td>Protecting the confidentiality and integrity of transmitted information applies to both internal and external networks, and any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical means or by logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a term for a wireless or fiber optics telecommunication system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-8 (1)</td>
<td>2</td>
<td>System and Communications Protection / Cryptographic Protection</td>
<td></td>
<td>Implement cryptographic mechanisms to (selection [one or more]: prevent unauthorized disclosure of information; detect changes in information) during transmission.</td>
<td>Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include SSL and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, challenge, and message authentication codes. SC-13 is used to specify the specific protocols, algorithms, and algorithm parameters to be implemented in each transaction path.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-8 (2)</td>
<td>2</td>
<td>System and Communications Protection / Transmission Confidentiality and Integrity / Pre- and Post-transmission Handling</td>
<td></td>
<td>Maintain the (selection [one or more]: confidentiality, integrity) of information during preparation for transmission and during reception.</td>
<td>Information can be either unilaterally or maliciously disclosed or modified during preparation for transmission or during reception, including during aggregation, at protocol transformation points, and during unpacking. Such unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control ID</td>
<td>Level</td>
<td>Control Name</td>
<td>Description</td>
<td>Restated Controls</td>
<td>Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>--------------</td>
<td>-------------</td>
<td>------------------</td>
<td>-------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-8 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Implement cryptographic mechanisms to protect message externals unless otherwise protected by assignment (organization-defined alternative physical controls). Cryptographic protection for message externals addresses protection from unauthorized disclosure of information. Cryptographic protection prevents the exploitation of message externals and applies to internal and external networks or links that may be visible to individuals who are not authorized users. Header and routing information is sometimes transmitted in clear text (i.e., unencrypted) because the information is not identified by organizations as having significant value or because encrypting the information can result in lower network performance or higher costs. Alternative physical controls include protected distribution systems.</td>
<td>SC-12, SC-13</td>
<td>Withdrawn: Incorporated into SC-8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-8 (4)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by assignment (organization-defined alternative physical controls). Concealing or randomizing communication patterns addresses protection from unauthorized disclosure of information. Communication patterns include frequency, period, predictability, and amount. Changes to communication patterns can reveal information having intelligence value especially when combined with other available information related to the missions and business functions of the organization. This control enhancement prevents the derivation of intelligence based on communications patterns and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Cryptographically linking and transmitting in continuous, fixed or random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical controls include protected distribution systems.</td>
<td>SC-12, SC-13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-8 (5)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Implement (assignment) organization-defined protected distribution system to (Select one or more): prevent unauthorized disclosure of information; detect changes to information during transmission; the purpose of a protected distribution system is to deter, detect and/or make difficult physical access to the communication lines carrying national security information.</td>
<td>SC-12, SC-13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-9</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Transmission Confidentiality</td>
<td>X</td>
<td>Withdrawn: Incorporated into SC-9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-10</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Network Dissemination</td>
<td>Terminate the network connection associated with a communications session at the end of the session or after assignment (organization-defined time period) of inactivity. Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP addresses or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network protocol types.</td>
<td>SC-17, SC-23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-11</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Trusted Path</td>
<td>a. Provide a (Selection: physically; logically) trusted trusted communications path for communications between the user and the trusted components of the system; and b. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: (Assignment: organization-defined security functions).</td>
<td>SC-10, SC-12, SC-13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-11 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Unsuitable Communications Path</td>
<td>a. Provide a trusted communications path that is indistinguishable from other communications paths; and b. If the trusted communications path is communicated between the (Assignment: organization-defined security functions) of the system and the user.</td>
<td>SC-17, SC-18, SC-25, SC-26, SC-30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-12</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Cryptographic Key Establishment and Management</td>
<td>Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: (Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction). Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations perform key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, specifying appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust actions are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems (NIST CMVP and NIST CAVP) provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.</td>
<td>SC-17, AU-9, AC-10, SI-6, SI-7, SE-4, SE-6, SE-14, SC-6, SC-11, SC-17, SC-20, SC-27, SC-40, SI-1, SI-7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-12 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Cryptographic Key Establishment and Management</td>
<td>Availability</td>
<td>Maintain availability of information in the event of the loss of cryptographic keys by users. Scratching of encryption keys in a common practice for ensuring availability in the event of loss of keys. A frequent paraphrase on an example of losing a cryptographic key.</td>
<td>AC-17, AU-9, AC-10, SI-6, SI-7, SE-4, SE-6, SE-14, SC-6, SC-11, SC-17, SC-20, SC-27, SC-40, SI-1, SI-7</td>
<td></td>
</tr>
<tr>
<td>SC-12 (2)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Cryptographic Key Establishment and Management</td>
<td>Symmetric Keys</td>
<td>Produce, control, and distribute symmetric cryptographic keys using (Selection: NIST SP 800-56A validated, NSA-approved) key management technology and processes.</td>
<td>SP 800-56A, SP 800-56B, and SP 800-56C provide guidance on cryptographic key establishment schemes and key derivation methods. [SP 800-57-1, SP 800-57-2, and SP 800-57-7] provide guidance on cryptographic key management.</td>
<td></td>
</tr>
<tr>
<td>SC-12 (3)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Cryptographic Key Establishment and Management</td>
<td>Asymmetric Keys</td>
<td>Produce, control, and distribute asymmetric cryptographic keys using (Selection: NSA-approved key management technology and processes; proportional keying material; DoS-approved or DoS-issued Medium Hardware Assurance PKI certificates; DoS-approved or DoS-issued Medium Middleware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements).</td>
<td>SP 800-56A, SP 800-56B, and SP 800-56C provide guidance on cryptographic key establishment schemes and key derivation methods. [SP 800-57-1, SP 800-57-2, and SP 800-57-7] provide guidance on cryptographic key management.</td>
<td></td>
</tr>
<tr>
<td>SC-12 (4)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Cryptographic Key Establishment and Management</td>
<td>Physical Control of Keys</td>
<td>Maintain physical control of cryptographic keys when stored information is encrypted by external service providers. For organizations using external service providers, for example, cloud service providers or data center providers, physical control of cryptographic keys provides additional assurance that information stored by such external providers is not subject to unauthorized disclosure or modification.</td>
<td>SC-17, AU-9, AC-10, SI-6, SI-7, SE-4, SE-6, SE-14, SC-6, SC-11, SC-17, SC-20, SC-27, SC-40, SI-1, SI-7</td>
<td></td>
</tr>
</tbody>
</table>

Page 88 of 108
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC-13</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Cryptographic Protection</td>
<td>a. Define the (assignment, organization-defined cryptographic use); and b. Implement the following types of cryptography required for each specified cryptographic use.</td>
<td>Cryptography can be employed to support a variety of security solutions including, the protection of classified and unclassified data, the provision of digital signatures and the enforcement of information separation.</td>
<td>AC-2, AC-3, AC-10, CP-12, MP-2, MP-4, MP-5, MP-6, MP-8, MP-9, MP-10, SI-12, SI-20, SI-23, SI-26, SI-40, SI-7, SI-10</td>
<td></td>
</tr>
<tr>
<td>SC-14</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Public Key Infrastructure</td>
<td>Public Key Infrastructure Certificates</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| SC-15      | 1     | System and Communications Protection | Collaborative Computing Devices and Applications | a. Collect data on users' systems, system components, or system services. b. Collect data on users' system components or system services. c. Collect data on users' system components or system services. d. Collect data on users' system components or system services. e. Collect data on users' system components or system services. f. Collect data on users' system components or system services. g. Collect data on users' system components or system services. h. Collect data on users' system components or system services. i. Collect data on users' system components or system services. j. Collect data on users' system components or system services. k. Collect data on users' system components or system services. l. Collect data on users' system components or system services. m. Collect data on users' system components or system services. n. Collect data on users' system components or system services. o. Collect data on users' system components or system services. p. Collect data on users' system components or system services. q. Collect data on users' system components or system services. r. Collect data on users' system components or system services. s. Collect data on users' system components or system services. t. Collect data on users' system components or system services. u. Collect data on users' system components or system services. v. Collect data on users' system components or system services. w. Collect data on users' system components or system services. x. Collect data on users' system components or system services. y. Collect data on users' system components or system services. z. Collect data on users' system components or system services. | | | }
null
Employ minimal functionality and information storage on the following system components:

- SC-25: System and Communications Protection | Protection
- SC-26: System and Communications Protection | Design
- SC-27: System and Communications Protection | Platform-Independent Applications
- SC-28: System and Communications Protection | Protection of Information at Rest

Platforms are combinations of hardware, firmware, and software components used to execute software applications. Platforms include operating systems, the underlying computer architectures, or both. Platform-independent applications are applications with the capability to execute on multiple platforms. Such applications promote portability and reusability on different platforms. Application portability and the ability to reconfigure on different platforms increase the availability of mission-essential functions within organizations in situations where systems with specific operating systems are under attack.

Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] that are changed [Assignment: organization-defined frequency].

- Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries and to deflect attacks away from the operational systems supporting organizational missions and business functions. Depending upon the specific usage of the遵义, consultation with the Office of the General Counsel before deployment may be needed.
- [Assignment: organization-defined safeguards]

- Increasing the diversity of information technologies within organizational systems reduces the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of online storage.

- Removing organizational information from online storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Organizations using cryptographic mechanisms also consider cryptographic key management solutions (see SC-12 and SC-13).

- Virtualization techniques can assist in isolating unauthorized software from confidential and integrity protection can be achieved, for example, by implementing Better Gross-Reed-Miller (BGMR) techniques.

- Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems]:

  - SC-29: System and Communications Protection | Protection of Information at Rest
  - SC-30: System and Communications Protection | Protection of Information at Rest
  - SC-31: System and Communications Protection | Protection of Information at Rest
  - SC-32: System and Communications Protection | Protection of Information at Rest

- Protect the [Selection (one or more): confidentiality; integrity; availability] of the following information at rest:

  - [Assignment: organization-defined information at rest]

- Protect the confidentiality and integrity of the following information at rest:

  - [Assignment: organization-defined information at rest]

- Protect the confidentiality, integrity, or availability of the following information at rest:

  - [Assignment: organization-defined information at rest]

- Protect the confidentiality, integrity, or availability of information at rest:

  - [Assignment: organization-defined information at rest]

- Protect the confidentiality, integrity, or availability of the following information at rest:

  - [Assignment: organization-defined information at rest]

- Protect the confidentiality, integrity, or availability of information at rest:

  - [Assignment: organization-defined information at rest]

- Protect the confidentiality, integrity, or availability of the following information at rest:

  - [Assignment: organization-defined information at rest]

- Protect the confidentiality, integrity, or availability of information at rest:

  - [Assignment: organization-defined information at rest]
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Description</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC-31 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td></td>
<td>Perform a covert channel analysis to identify covert communications within the system that are potential avenues for covert access (e.g., storage, timing) channels; and 3. Estimate the maximum bandwidth of these channels. Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for uncontrolled information flows across security domains, for example, in the case of systems containing export-controlled information and having connections to external networks (e.g., networks that are not controlled by organizations). Covert channel analysis is also useful for multilevel secure systems, multiple security level systems, and cross-domain systems.</td>
<td>SC-26, SC-30, SI-11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-32 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td></td>
<td>Test a subset of the identified covert channels to determine the channels that are exploitable. None.</td>
<td></td>
<td>SC-26, SI-11</td>
<td></td>
</tr>
<tr>
<td>SC-32 (2)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td></td>
<td>Reduce the maximum bandwidth for identified covert channels (e.g., storage, timing) channels to assignment: organization-defined values. The complete elimination of covert channels, especially covert timing channels, is usually not possible without significant performance impacts.</td>
<td></td>
<td>SC-26, SI-11</td>
<td></td>
</tr>
<tr>
<td>SC-32 (3)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td></td>
<td>Reduce the maximum bandwidth for identified covert channels (e.g., storage, timing) channels to assignment: organization-defined values. The complete elimination of covert channels, especially covert timing channels, is usually not possible without significant performance impacts.</td>
<td></td>
<td>SC-26, SI-11</td>
<td></td>
</tr>
<tr>
<td>SC-32 (4)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td></td>
<td>Partition the system into [Assignment: organization-defined system components] residing in separate [Selection: physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components]. System partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components. Physical separation includes physically distinct components in separate roles in the same room, critical components in separate rooms, and geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.</td>
<td>SC-26, SC-30, SC-13, SC-27, SC-36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC-32 (5)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td></td>
<td>Partition privileged functions into separate physical domains. Privileged functions operating in a single physical domain may represent a single point of failure if that domain becomes compromised or experiences a denial of service.</td>
<td></td>
<td>SC-26, SI-11</td>
<td></td>
</tr>
<tr>
<td>SC-33 (1)</td>
<td>3</td>
<td>System and Communications Protection</td>
<td>X</td>
<td>Transaction: Organization-Defined Integrity</td>
<td>System components that proactively seek to identify network-based malicious code or malicious websites. External malicious code identification differs from defenses in SC-26 in that the components actively probe networks, including the Internet, in search of malicious code contained on external websites. Like decoys, the use of external malicious code-identification techniques requires some supporting isolation measures to ensure that any malicious code discovered during the search and subsequently executed does not affect organizational systems. Virtualization is a common technique for achieving such isolation.</td>
<td>SC-20, SC-44, SI-3, SI-4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawal</th>
<th>Control Text</th>
<th>Document</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC-36</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Distributed</td>
<td>Processing and Storage</td>
<td>(distribute the following processing and storage components across multiple (selection: physical locations, logical domains): (assignment: organization-defined processing and storage components):</td>
<td>Distributed processing and storage across multiple physical locations or logical domains provides a degree of redundancy or overlay for organizations. The redundancy and overlap increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. The use of distributed processing and storage does not constitute a single primary processing or storage location. Therefore, it allows for parallel processing and storage.</td>
<td>PE-3, PE-7, PE-8, SI-12</td>
</tr>
<tr>
<td>SC-36 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Distributed</td>
<td>Processing and Storage</td>
<td></td>
<td>(a) Employ technical techniques to identify potential faults, errors, or compromises to the following processing and storage components: (assignment: organization-defined distributed processing and storage components); and (b) take the following actions in response to identified faults, errors, or compromises: (assignment: organization-defined actions):</td>
<td>Distributed processing and/or storage may be used to reduce opportunities for adversaries to compromise the confidentiality, integrity, or availability of organizational information and systems. However, distributed processing and/or storage components does not prevent adversaries from compromising one or more of the components. Polling compares the processing results and/or storage content from the distributed components and subsequently votes on the outcomes. Polling identifies potential faults, compromises, or errors in the distributed processing and storage components. Polling techniques may also be applied to processing and storage components that are not physically distributed</td>
</tr>
<tr>
<td>SC-36 (2)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Distributed</td>
<td>Processing and Storage</td>
<td>(synchronization the following appliance systems or system components: (assignment: organization-defined appliance systems or system components):</td>
<td>SC-36 and CP-8 require the exploitation of systems or system components in distributed locations. Synchronization of duplicated and redundant services and data helps to ensure that information contained in the distributed locations can be used in the mission or business functions of organizations, as needed.</td>
<td>CP-3</td>
</tr>
<tr>
<td>SC-37</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Out-of-</td>
<td>Band Channels</td>
<td>Employ the following out-of-band channels for the physical delivery or electronic transmission of (assignment: organization-defined information, system components, or devices): (assignment: organization-defined out-of-band channels):</td>
<td>Out-of-band channels include local linkwork accessible to systems: network paths physically separate from network paths used for operational traffic, or non-routeable paths such as the US Postal Service. The use of out-of-band channels is contrasted with the use of in-band channels (i.e., the same channel) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability or exposure as in-band channels. Therefore, the confidentiality, integrity, or availability compromises of in-band channels will not compromise or adversely affect the out-of-band channels. Organizations may employ out-of-band channels in the delivery or the transmission of organizational items, including identifying and authenticating, cryptographic key management information, system and data backups, configuration management changes for hardware, firmware, or software, security updates, maintenance information, and malicious code protection updates.</td>
<td>AC-1, CA-2, CA-5, CM-7, IK-2, IK-4, IK-5, MI-4, SI-12, SI-14, SI-15</td>
</tr>
<tr>
<td>SC-37 (2)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Out-of-</td>
<td>Band Channels</td>
<td></td>
<td></td>
<td>Employ (assignment: organization-defined controls) to ensure that only (assignment: organization-defined individuals or systems) review the following information, system components, or devices: (assignment: organization-defined information, system components, or devices):</td>
</tr>
<tr>
<td>SC-38</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Operations</td>
<td>Security</td>
<td>Employ the following operations security controls to protect key organizational information throughout the system development life cycle: (assignment: organization-defined operations security controls):</td>
<td>Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and the application of appropriate countermeasures. OPSEC controls are applied to organizational systems and the environments in which those systems operate. OPSEC controls protect the confidentiality of information, including limiting the sharing of information with suppliers and potential suppliers of system components and services, and with other non-organizational elements and individuals. Information critical to organizational missions and business functions includes user identities, element uses, suppliers, supply chain processes, functional requirements, security requirements, system design specifications, testing and evaluation protocols, and security control implementation details.</td>
<td>AC-1, AC-4, AC-6, AC-31, CA-4, SC-2, SC-3, SI-6</td>
</tr>
<tr>
<td>SC-39</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Process</td>
<td>Isolation</td>
<td>Maintain a separate execution domain for each executing system process.</td>
<td>Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has an 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. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially malicious software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-threaded processor technologies.</td>
<td>AC-1, SC-5</td>
</tr>
<tr>
<td>SC-39 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Process</td>
<td>Isolation</td>
<td></td>
<td>Implement hardware separation mechanisms to facilitate process isolation.</td>
<td>Hardware-based separation of system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Hardware separation mechanisms include hardware memory management.</td>
</tr>
<tr>
<td>SC-39 (2)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Process</td>
<td>Isolation</td>
<td></td>
<td>Maintain a separate execution domain for each thread in (assignment: organization-defined multi-threaded processing):</td>
<td>None.</td>
</tr>
<tr>
<td>SC-40</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Wireless</td>
<td>Link Protection</td>
<td>Protect external and internal (assignment: organization-defined wireless links) from the following signal parameter attacks: (assignment: organization-defined types of signal parameter attacks or references to sources for such attacks):</td>
<td>Wireless link protection applies to internal and external wireless communication links that are visible to individuals who are not authorized system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or spoof system users. Protection of wireless links reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may be possible to implement this control.</td>
<td>AC-18, SC-5</td>
</tr>
<tr>
<td>SC-40 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Wireless</td>
<td>Link Protection</td>
<td></td>
<td>Implement cryptographic mechanisms that achieve (assignment: organization-defined level of protection) against the effects of intentional electromagnetic interferences:</td>
<td>Implementation of cryptographic mechanisms for electromagnetic interference protection against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The implementation of cryptographic mechanisms may also considerably mitigate the effects of unintentional jamming due to interference from legitimate transmitters operating in the same spectrum. Mission requirements, acquisition objectives, and allowable live, executive order, directives, regulations, policies, and standards determine levels of wireless availability, cryptography reward, or performance.</td>
</tr>
</tbody>
</table>
### System and Communications Protection

#### SC-40 (1) System and Communications Protection | Wireless Link Protection | Sensor

- **Implementation:** Categorize mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve intrusive or manipulative communications deception based on signal parameters.

#### SC-41 1 System and Communications Protection | Detonation

- **Implementation:** Categorize mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve intrusive or manipulative communications deception based on signal parameters.

#### SC-42 1 System and Communications Protection | Usage

- **Implementation:** Categorize mechanisms to prevent the identification of assignments of organization-defined wireless transmitters, by using the transmitter signal parameters.

### System and Communications Protection

#### SC-42 (1) System and Communications Protection | Sensor

- **Implementation:** Categorize mechanisms to prevent the identification of organization-defined sensors by using the transmitter signal parameters.

#### SC-42 (2) System and Communications Protection | Wireless

- **Implementation:** Categorize mechanisms to prevent the identification of organization-defined wireless transmitters, by using the transmitter signal parameters.

### System and Communications Protection

#### SC-42 (3) System and Communications Protection | Wireless

- **Implementation:** Categorize mechanisms to prevent the identification of organization-defined wireless transmitters, by using the transmitter signal parameters.

### System and Communications Protection

#### SC-42 (4) System and Communications Protection | Wireless

- **Implementation:** Categorize mechanisms to prevent the identification of organization-defined wireless transmitters, by using the transmitter signal parameters.

### System and Communications Protection

#### SC-42 (5) System and Communications Protection | Wireless

- **Implementation:** Categorize mechanisms to prevent the identification of organization-defined wireless transmitters, by using the transmitter signal parameters.

### System and Communications Protection

#### SC-43 1 System and Communications Protection | System and Communications Protection | Detonation

- **Implementation:** Categorize mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve intrusive or manipulative communications deception based on signal parameters.

### System and Communications Protection

#### SC-43 (1) System and Communications Protection | System and Communications Protection | Detonation

- **Implementation:** Categorize mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve intrusive or manipulative communications deception based on signal parameters.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC-46</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Gross Domain Policy Enforcement</td>
<td>Implement a policy enforcement mechanism (selection: physically, logically) between the physical and/or network interfaces for the connecting security domains.</td>
<td>For logical policy enforcement mechanisms, organizations avoid creating a logical gap between interfaces to prevent the ability to bypass the policy enforcement mechanism. For physical policy enforcement mechanisms, the robustness of physical isolation affected by the physical implementation of policy enforcement to preclude the presence of logical control pathways generating the security boundary may be needed.</td>
<td>A/C-4, A/C-7</td>
<td></td>
</tr>
<tr>
<td>SC-47</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Communications Path Diversity</td>
<td>Establish [Assignment: organization-defined alternate communications paths] for system operations or organizational command and control.</td>
<td>An incident, whether adversarial- or non-adversarial-based, can disrupt established communications paths used for system operations and organizational command and control. The inability of organizational officials to obtain timely information about disruptions or to provide timely direction to operational elements can impact the organization’s ability to respond in a timely manner to such incidents. Establishing alternate communications paths for command and control purposes, including designing alternative decision-makers if primary decision-makers are unavailable and establishing the extent and limitations of their actions, can greatly facilitate the organization’s ability to continue to operate and take appropriate actions during an incident.</td>
<td>C/F-2, C/F-8</td>
<td></td>
</tr>
<tr>
<td>SC-48</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Sensor Relocation</td>
<td>Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances:</td>
<td>Adversaries may take various paths and use different approaches as they move laterally through an organization (including its systems) to reach their target or as they attempt to exfiltrate information from the organization. The organization offers only a limited set of monitoring and detection capabilities and may be focused on the critical or likely infiltration or exfiltration paths. By using communications paths that the organization typically does not monitor, the adversary can increase his chances of achieving his desired goals. By relocating the sensors or monitoring capabilities to new locations, the organization can improve the adversary’s ability to achieve his goals. The relocation of the sensors or monitoring capabilities might be done based on threat information the organization has acquired or was able to confirm the adversary and make its lateral transition through the system or organization more challenging.</td>
<td>A/C-2, SC-7, GC-4</td>
<td></td>
</tr>
<tr>
<td>SC-48 (1)</td>
<td>2</td>
<td>System and Communications Protection</td>
<td>Sensor Relocation</td>
<td>Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances:</td>
<td>None.</td>
<td>None.</td>
<td></td>
</tr>
<tr>
<td>SC-49</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Hardware-enforced Separation and Policy Enforcement</td>
<td>Implement hardware-enforced and policy enforcement mechanisms between [Assignment: organization-defined security domains].</td>
<td>System owners may require additional strength of mechanism and robustness to ensure domain separation and policy enforcement for specific types of threats and environments of operation. Hardware-enforced separation and policy enforcement provide greater strength of mechanism than software-enforced separation and policy enforcement.</td>
<td>A/C-4, SA-8, SC-50</td>
<td></td>
</tr>
<tr>
<td>SC-50</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Software-enforced Separation and Policy Enforcement</td>
<td>Implement software-enforced and policy separation mechanisms between [Assignment: organization-defined security domains].</td>
<td>System owners may require additional strength of mechanism and robustness to ensure domain separation and policy enforcement (e.g., filtering) for specific types of threats and environments of operation.</td>
<td>A/C-4, AC-6, SA-8, SC-50, SC-43, SC-49</td>
<td></td>
</tr>
<tr>
<td>SC-51</td>
<td>1</td>
<td>System and Communications Protection</td>
<td>Operational and Internet-based Technologies</td>
<td>Implement the following controls on [Assignment: organization-defined Operational Technology (OT)] systems:</td>
<td>Operational technology (OT) represents a variety of hardware, software, and firmware components of a system used to detect or cause changes in physical processes through the direct control and monitoring of physical devices. Examples include distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs). The term operational technology is used to denote the differences between industrial control systems (ICS) that are typically found in manufacturing and power plants and the information technology (IT) systems that typically support transactional data processing applications. The term Internet of Things (IoT) is used to describe the network of devices, (e.g., vehicles, medical devices, wearables, and home appliances) that are capable of communicating/interacting with one another or with other devices and systems to exchange information, services, and management services. The recent convergence of OT and IT, producing cyber-physical systems, increases the attack surface of organizations significantly and poses unique threats that are challenging to address. Fortunately, most of the current generation of IoT, OT and ISF devices are not designed with security in mind. Communicating with off-the-shelf devices is possible, but not encouraged. It is not necessary to provide the necessary security, nor are they designed, and are not logged. As a result, these devices pose a significant cyber threat. In some instances, gaps in OT, ISF, and IoT security capabilities may be addressed by employing intermediary devices that can provide encryption, authentication, scanning, and isolating capabilities, and protect the devices from being accessed from the Internet. But such integrating options are not always available. The situation is further complicated because some of the OT/IT/IoT devices are needed for essential operations, and it is not acceptable that such devices are isolated from the systems to reduce the susceptibility to hostile cyber attacks.</td>
<td>A/C-4, AC-6, SA-8, SC-50, SC-43, SC-49</td>
<td></td>
</tr>
</tbody>
</table>

I-1 System and Information Integrity | Policy and Procedures | 
| I-1 | System and Information Integrity | Policy and Procedures | 
| I-2 | System and Information Integrity | Policy and Procedures | 
| I-3 | System and Information Integrity | Policy and Procedures | 
| I-4 | System and Information Integrity | Policy and Procedures | 

This control addresses policy and procedures for the controls in the I-1 family implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures help provide security and privacy assurance. Therefore, it is important that security and privacy programs collaborate as they development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for systems-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complete scope of the organization. Procedures can be established for security and privacy programs and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Controlling controls does not constitute an organizational policy or procedure. | PM-0, Ps-8, SA-8, U-3 |
- a. Identify, report, and correct system flaws; and
- b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organization-wide management and implementation policies and procedures.
- c. Configure malicious code protection mechanisms to:
  - 1. Perform periodic scans of the system (assignment: organization-defined frequency) and real-time scans of new and updated versions have been installed.
  - 2. [Selection (one or more): block malicious code; quarantine malicious code; take corrective actions; automatically update malicious code protection mechanisms.]

- 2. Perform periodic scans of the system (assignment: organization-defined frequency) and real-time scans of new and updated versions have been installed.
- 3. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

- 3. System and Information Integrity / Malicious Code Protection
- a. Implement [selection (one or more): signature-based non-signature-based malicious code protection mechanisms on system entry and exit points to detect and eradicate malicious code;]
- b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.
- c. Configure malicious code protection mechanisms to:
  - 1. Perform periodic scans of the system (assignment: organization-defined frequency) and real-time scans of new and updated versions have been installed.
  - 2. [Selection (one or more): block malicious code; quarantine malicious code; take corrective actions; automatically update malicious code protection mechanisms.]

- System entry and exit points include firewalls, remote-access servers, web proxies, computer servers, and mail servers. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be recorded in various formats controllable through compressed or hidden files, or hidden in the file names of technologies such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code can also be encoded in various formats, such as scripts, shell scripts, and Java applets.

- Malicious code protection mechanisms include both signature-based and non-signature-based technologies. Signature-based detection mechanisms include automated intelligence techniques that can identify and extract, analyze, and describe the characteristics or behavior of malicious code. Non-signature-based detection mechanisms include artificial intelligence techniques that can detect malicious code by understanding the context in which it appears. Non-signature-based detection mechanisms also include the use of heuristics to detect malicious code. Non-signature-based detection mechanisms can be effective in preventing execution of unauthorized code. Malicious code may be present in commercial off the shelf software and in custom-built software and may include logic bombs, back doors, and other types of attacks that could affect organizational missions and business functions.

- Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from these flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. Organizations determine the time it takes on average to correct system flaws after such flaws have been discovered and, subsequently, establish organizational benchmarks, i.e., time frames for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

- 3.1 (1) System and Information Integrity / Malicious Code Protection
- a. Implement [selection (one or more): signature-based non-signature-based malicious code protection mechanisms on system entry and exit points to detect and eradicate malicious code;]
- b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.
- c. Configure malicious code protection mechanisms to:
  - 1. Perform periodic scans of the system (assignment: organization-defined frequency) and real-time scans of new and updated versions have been installed.
  - 2. [Selection (one or more): block malicious code; quarantine malicious code; take corrective actions; automatically update malicious code protection mechanisms.]

- System entry and exit points include firewalls, remote-access servers, web proxies, computer servers, and mail servers. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be recorded in various formats controllable through compressed or hidden files, or hidden in the file names of technologies such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code can also be encoded in various formats, such as scripts, shell scripts, and Java applets.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI-3 (8) 2</td>
<td>System and Information Integrity</td>
<td>Malicious Code Analysis</td>
<td>System Monitoring</td>
<td>Implement (Assignment: organization-defined mechanisms) to authenticate (Assignment: organization-defined remote command);</td>
</tr>
<tr>
<td>SI-4 (12) 2</td>
<td>System and Information Integrity</td>
<td>Malicious Code Analysis</td>
<td>System Monitoring</td>
<td>Provide (Assignment: organization-defined system monitoring information) to (Assignment: organization-defined personnel or roles) as needed; (Assignment: organization-defined frequency);</td>
</tr>
<tr>
<td>SI-4 1</td>
<td>System and Information Integrity</td>
<td>System Monitoring</td>
<td>System Monitoring</td>
<td>a. Monitor the system to detect:</td>
</tr>
<tr>
<td>SI-4 2</td>
<td>System and Information Integrity</td>
<td>System Monitoring</td>
<td>System Monitoring</td>
<td>b. Identify unauthorized use of the system through the following techniques and methods: (Assignment: organization-defined detection activities);</td>
</tr>
<tr>
<td>SI-4 3</td>
<td>System and Information Integrity</td>
<td>System Monitoring</td>
<td>System Monitoring</td>
<td>c. Invoke internal monitoring capabilities or deploy monitoring devices:</td>
</tr>
</tbody>
</table>

**Notes**

- The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., motives, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates effective organizational responses to current and future threats. Organizations can conduct malicious code analysis by employing reverse engineering techniques or by monitoring the behavior of executing code.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Remediated Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI-4 (17)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td>0</td>
<td>(a) Notify [Assignment: organization-defined incident response personnel] identified by role and/or by risk of detected suspicious events; and (b) take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events].</td>
<td>Least-disruptive actions include initiating requests for human responses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI-4 (18)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI-4 (19)</td>
<td>2</td>
<td>System and Information Integrity / Protection of Monitoring Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI-4 (20)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>Test intrusion monitoring tools and mechanisms [Assignment: organization-defined frequency].</td>
<td>Testing intrusion monitoring tools and mechanisms is necessary to ensure that the tools and mechanisms are operating correctly and continue to satisfy the monitoring objectives of organizations. The frequency and depth of testing depend on the types of tools and mechanisms used by organizations and the methods of deployment.</td>
<td>CP-3</td>
<td></td>
</tr>
<tr>
<td>SI-4 (21)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>Make provisions so that [Assignment: organization-defined encrypted communications traffic] [is a visitor to [Assignment: organization-defined system-monitoring tools and mechanisms]].</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI-4 (22)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with privacy or security implications occur: [Assignment: organization-defined activities that trigger alerts].</td>
<td>Organizational personnel on the systems and mechanisms for system administration, misuse or business owners, system owners, senior agency information security officers, senior agency officials by privacy, system security officers, or privacy officers. This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. It is intended to the alerts generated by systems in SI-4(21) that focus on information elements that are internal to the systems such as audit records, the sources of information for the information of this focus on other elements such as suspicious activity reports and reports on potential insider threats.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI-4 (23)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>(a) Analyze communications traffic and event patterns for the system; (b) Develop profiles representing common traffic and event patterns; and (c) Use the traffic and event profiles in tuning system-monitoring devices.</td>
<td>Identifying and understanding system communications traffic and event patterns helps organizations provide useful information to system monitoring tools to more effectively identify suspicious or anomalous events and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.</td>
<td>AC-18, IA-3</td>
<td></td>
</tr>
<tr>
<td>SI-4 (24)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td>Examine failed审计 attempts and to detect attack attempts and potential compromise or breaches to the system.</td>
<td>Whiteline signals may require additional organizational analysis. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Whiteline signals are not limited to those areas where facilities contain systems, but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational networks.</td>
<td>AC-18</td>
</tr>
<tr>
<td>SI-4 (25)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI-4 (26)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td>Correlate information from monitoring tools and mechanisms employed throughout the system.</td>
<td>Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation, including malicious code protection software, host monitoring, and network monitoring, can provide an organization-wide monitoring view and may reveal otherwise uncorrelated attacks. Understanding capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the utility of information generated by these tools and mechanisms can help organizations to identify, operate, and maintain effective monitoring programs. Correlation of monitoring information is especially important during the transition from older to newer technologies (e.g., migrating from third-to fifth-generation network protocols).</td>
<td>AC-4</td>
</tr>
<tr>
<td>SI-4 (27)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td>Correlate information from marketing physical, cyber, and supply chain activities to achieve integrated, organization-wide, and integrated awareness.</td>
<td>Correlating monitoring information from a more diverse set of information sources helps to achieve integrated awareness. Integrated awareness can be a combination of physical, cyber, and supply chain monitoring activities that enhances the visibility of organization to more quickly detect unauthorized attempts and investigate the methods and tactics employed by attackers. In contrast to (SI-4(26)) that correlates the various cyber monitoring information, this control enhancement correlates the information of monitoring information from a more diverse set of information sources.</td>
<td>AC-16, RI-6</td>
</tr>
<tr>
<td>SI-4 (28)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td>Examine unauthorized communications traffic at external interfaces to the system and the following internal points to detect count of unusual information [Assignment: organization-defined monitoring points within the system].</td>
<td>Examination of increased risk from individual can be obtained from different sources, such as audit records, network monitoring tools and mechanisms that typically work in isolation, including malicious code protection software, host monitoring, and network monitoring.</td>
<td>AC-18</td>
</tr>
<tr>
<td>SI-4 (29)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td>Implement the following additional monitoring of privileged users [Assignment: organization-defined additional monitoring].</td>
<td>Privileged users have access to more sensitive information, including security-related information, that is not general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions.</td>
<td>AC-18</td>
</tr>
<tr>
<td>SI-4 (30)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td>Implement the following additional monitoring of privileged users [Assignment: organization-defined additional monitoring].</td>
<td>During probationary periods, employees do not have permanent employment status within organizations. Without such status and having access to information that is resident on the systems, additional monitoring can help identify any potentially malicious activity or inappropriate behavior.</td>
<td>AC-18</td>
</tr>
<tr>
<td>SI-4 (31)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td>Implement the following additional monitoring of privileged users [Assignment: organization-defined additional monitoring].</td>
<td>During probationary periods, employees do not have permanent employment status within organizations. Without such status and having access to information that is resident on the systems, additional monitoring can help identify any potentially malicious activity or inappropriate behavior.</td>
<td>AC-18</td>
</tr>
<tr>
<td>SI-4 (32)</td>
<td>2</td>
<td>System and Information Integrity / System Monitoring</td>
<td></td>
<td>System and Information Integrity / System Monitoring</td>
<td>Implement the following additional monitoring of privileged users [Assignment: organization-defined additional monitoring].</td>
<td>During probationary periods, employees do not have permanent employment status within organizations. Without such status and having access to information that is resident on the systems, additional monitoring can help identify any potentially malicious activity or inappropriate behavior.</td>
<td>AC-18</td>
</tr>
</tbody>
</table>

Notes: Withdrawn: Incorporated into SI-4.
### System and Information Integrity

**SI-4 (23)** 2 System and Information Integrity | System Monitoring 
Implement the following host-based monitoring mechanisms at [assignment: organization-defined system components]; [assignment: organization-defined host-based monitoring mechanisms].

System components where host-based monitoring can be implemented include servers, potential containers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.

**SI-4 (24)** 2 System and Information Integrity | System Monitoring
Discover, collect, and distribute to [assignment: organization-defined personal or roles] Indicators of compromise provided by [assignment: organization-defined sources].

Indicators ofcompromise (IOCs) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs can include the creation of registry key values. IOCs for network traffick include Universal Resource Locator (URL), protocol elements that identify malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploits or attacks. Threat indicators, signatures, metrics, techniques, and procedures, and other indicators of compromise may be available across government and non-government organizations including Federal Computer Incident Response Teams, Defense Industrial Base Cybersecurity Information Sharing Program, and CIRT Coordination Center.

**SI-4 (24)** 2 System and Information Integrity | System Monitoring
Implement automated Network Traffic Analysis tools to enable visibility into network traffic at external and key external system boundaries to optimize the effectiveness of monitoring devices.

Automated traffic, symmetric routing architectures, capacity and latency limitations, and transitioning from older to newer technologies (e.g., IPv6 to IPv4 network protocol transition) may result in blind spots for organizations when analyzing network traffic. Collecting, aggregating, pre-processing and distributing only relevant traffic to monitoring devices can improve efficiency and use of the traffic and system traffic analysis.

### System and Information Integrity

**SI-6 (3)** 2 System and Information Integrity | Security and Privacy Function Verification
Implement automated mechanisms to support the management of distributed security and privacy function verification.

The use of automated mechanisms to support the management of distributed function verification helps to ensure the integrity, timeliness, competency, and efficacy of such testing.

**SI-6 (4)** 2 System and Information Integrity | Security and Privacy Function Verification
Perform integrity checks of [assignment: organization-defined security and privacy functions].

Security-relevant events include the identification of new threat to which organizational systems are susceptible, and the instantiation of new hardware, software, or firmware. Organizational personnel with potential concern in the results of verification of security function include system security officers, senior agency information security officers, and senior agency officials for privacy.

**SI-5 (1)** 2 System and Information Integrity | Security and Privacy Function Verification
Broadcast security alert and advisory information throughout the organization using [assignment: organization-defined automated mechanisms].

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct stake in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of organizational security and privacy risk, including the degree of noncompliance.

**SI-5 (2)** 2 System and Information Integrity | Security and Privacy Function Verification
Implement automated mechanisms to support the management of distributed security and privacy function verification.

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct stake in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of organizational security and privacy risk, including the degree of noncompliance.

### System and Information Integrity

**SI-7 (1)** 2 System and Information Integrity | Security and Privacy Function Verification
Implement automated mechanisms to support the management of distributed security and privacy function verification.

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct stake in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of organizational security and privacy risk, including the degree of noncompliance.

**SI-7 (2)** 2 System and Information Integrity | Security and Privacy Function Verification
Perform integrity checks of [assignment: organization-defined security and privacy functions].

Security-relevant events include the identification of new threat to which organizational systems are susceptible, and the instantiation of new hardware, software, or firmware. Organizational personnel with potential concern in the results of verification of security function include system security officers, senior agency information security officers, and senior agency officials for privacy.

**SI-7 (3)** 2 System and Information Integrity | Security and Privacy Function Verification
Implement automated mechanisms to support the management of distributed security and privacy function verification.

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct stake in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of organizational security and privacy risk, including the degree of noncompliance.

**SI-7 (4)** 2 System and Information Integrity | Security and Privacy Function Verification
Perform integrity checks of [assignment: organization-defined security and privacy functions].

Security-relevant events include the identification of new threat to which organizational systems are susceptible, and the instantiation of new hardware, software, or firmware. Organizational personnel with potential concern in the results of verification of security function include system security officers, senior agency information security officers, and senior agency officials for privacy.

**SI-7 (5)** 2 System and Information Integrity | Security and Privacy Function Verification
Implement automated mechanisms to support the management of distributed security and privacy function verification.

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct stake in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of organizational security and privacy risk, including the degree of noncompliance.

**SI-7 (6)** 2 System and Information Integrity | Security and Privacy Function Verification
Perform integrity checks of [assignment: organization-defined security and privacy functions].

Security-relevant events include the identification of new threat to which organizational systems are susceptible, and the instantiation of new hardware, software, or firmware. Organizational personnel with potential concern in the results of verification of security function include system security officers, senior agency information security officers, and senior agency officials for privacy.

**SI-7 (7)** 2 System and Information Integrity | Security and Privacy Function Verification
Implement automated mechanisms to support the management of distributed security and privacy function verification.

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct stake in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of organizational security and privacy risk, including the degree of noncompliance.
Si-7 (2) 2 System and Information Integrity | Software, Firmware, and Information Integrity | Cryptographic Protection
Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

- Cryptographic mechanisms used to protect integrity include digital signatures and the comparison and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Organizations employing cryptographic mechanisms also consider cryptographic key management solutions (see SC-12 and SC-13).

- Si-7 (7) 2 System and Information Integrity | Software, Firmware, and Information Integrity | Software, Firmware, and Information Integrity | Code Execution in Protected Environments
Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].

- Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code-signing is an effective method to protect against malicious code. Organizations employing cryptographic mechanisms also consider cryptographic key management solutions (see SC-12 and SC-13).

- Si-7 (12) 2 System and Information Integrity | Software, Firmware, and Information Integrity | Time Limit on Processes Execution Without Supervision
Prohibit processes from executing without supervision for more than [Assignment: organization-defined time-period].

- This control enhancement addresses processes for which typical or normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes timers on operating systems, automated responses, or manual oversight and response when system anomalies occur.

- Si-7 (13) 2 System and Information Integrity | Software, Firmware, and Information Integrity | Integrity Verification
Require that the integrity of the following user-installed software be verified prior to execution: [Assignment: organization-defined user-installed software].

- Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or executing code that contains errors.

- Si-7 (14) 2 System and Information Integrity | Software, Firmware, and Information Integrity | Library or Machine Executable Code
Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].

- Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code-signing is an effective method to protect against malicious code. Organizations employing cryptographic mechanisms also consider cryptographic key management solutions (see SC-12 and SC-13).

- Si-8 1 System and Information Integrity | Spam Protection
a. Employ spam protection mechanisms at system entry and out points to detect and act on unsolicited messages; and
b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

- System entry and out points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web access. Spam protection mechanisms include signature definitions.

- Si-9 (2) 2 System and Information Integrity | Software Protection | Control Management
Centrally manage spam protection mechanisms.

- Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection solutions.

- Si-9 (3) 2 System and Information Integrity | Software Protection | Continuous Learning Capability
Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communication traffic.

- Learning mechanisms include Bayesian filters that require user input identifying specific traffic as spam or legitimate by updating parameter values and thereby more accurately regulating types of traffic.

- Si-9 (4) 2 System and Information Integrity | Information Input Restrictions
X

(a) Generate error messages that provide information necessary for corrective actions without revealing sensitive information. For example, fields that are invalid inputs may display a message like: ‘Invalid input detected in field X: Character 'Y' is not allowed.’

(b) Audit the use of error messages in production environments.

(c) Provide a manual override capability for input validation.

(d) Restrict the use of manual override capability to only those systems that have implemented a manual override capability for input validation.

(e) Prevent untrusted data injections. Untrusted data injections may be prevented using, for example, a parameterized interface (output escaping).

(f) Account for timing interactions among system components in determining appropriate responses for invalid inputs.

(g) Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

(h) Check the validity of the following information inputs: [Assignment: organization-defined information inputs].

(i) Specify to the system the structure and the content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details, erroneous input attempts with passwords intentionally entered as the username, messages or locations information that can be derived from, if not stored explicitly, the information recorded; and personally identifiable information such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

(j) Audit the use of error messages in production environments.

(k) Provide a manual override capability for input validation.

(l) Restrict the use of manual override capability to only those systems that have implemented a manual override capability for input validation.

(m) Prevent untrusted data injections. Untrusted data injections may be prevented using, for example, a parameterized interface (output escaping).

(n) Account for timing interactions among system components in determining appropriate responses for invalid inputs.

(o) Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

(p) Check the validity of the following information inputs: [Assignment: organization-defined information inputs].

(q) Specify to the system the structure and the content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details, erroneous input attempts with passwords intentionally entered as the username, messages or locations information that can be derived from, if not stored explicitly, the information recorded; and personally identifiable information such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

(r) Prevent untrusted data injections. Untrusted data injections may be prevented using, for example, a parameterized interface (output escaping).

(s) Account for timing interactions among system components in determining appropriate responses for invalid inputs.

(t) Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

(u) Check the validity of the following information inputs: [Assignment: organization-defined information inputs].

(v) Specify to the system the structure and the content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details, erroneous input attempts with passwords intentionally entered as the username, messages or locations information that can be derived from, if not stored explicitly, the information recorded; and personally identifiable information such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.
SI-13 1 System and Information Integrity | Predictable Failure Prevention

(a) Determine mean time to failure (MTTF) for the following system components in specific environments of operation: 
   (Assignment: organization-defined system components and services), and

(b) Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: 
   (Assignment: organization-defined MTTF substitution criteria).

While MTTF is primarily a reliability issue, this control addresses potential failures of system components that provide security capability. Failure rates reflect installation-specific consideration, not industry-average. Organizations define the criteria for substitution of system components based on the MTTF value with consideration for resulting potential harm from component failures. Transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capability. This includes preservation of system state variables. Standby components remain available at all times except for maintenance issues or recovery failures in progress.

SI-13 (1) 2 System and Information Integrity | Predictable Failure Prevention / Transferring Component Responsibilities

Take system components out of service by transferring component responsibilities to substitute components no later than: 
   (Assignment: organization-defined fraction or percentage) of mean time to failure.

Transferring primary system component responsibilities to substitute components prior to primary component failure is important to reduce the risk of degraded or destabilized mission or business operations. Making such transfers based on a percentage of mean time to failure allows organizations to be proactive based on their risk tolerance. However, premature replacement of system components can result in increased cost of system operations.

SI-13 (2) 2 System and Information Integrity | Predictable Failure Prevention / Time Limit on Process Execution Without Assurance

Manually initiate transfers between active and standby system components when the use of the active component reaches: 
   (Assignment: organization-defined percentage) of the mean time to failure.

For example, if the MTTF of a system component is one hundred days and the organization-defined percentage is ninety percent, the manual transfer would occur after ninety days.

SI-13 (3) 2 System and Information Integrity | Predictable Failure Prevention / Manual Transfer Between Components

If a system component or facility is damaged or destroyed:

(a) Ensure that the standby components are successfully and transparently installed within: 
   (Assignment: organization-defined time period), and

(b) On detection (see or hear, activate, or observe): 
   (Assignment: organization-defined alarm); automatically shut down the systems; 
   (Assignment: organization-defined actions).

Failover refers to the automatic switchover to an alternate system upon the failure of the primary system. Failover capability includes incorporating minimal system operations at alternate processing sites or periods or data mirroring at replicate intervals defined by recovery time-period of organization.

SI-14 1 System and Information Integrity | Non-persistence

Implement non-persistent: 
   (Assignment: organization-defined system components and services) that are initiated in a known state and terminated: 
   (Selection: [one or more] upon end of session or use; periodically at: 
   (Assignment: organization-defined frequency).

Non-persistent system components and services can be useful in minimizing the risk to an organization from compromised resources, preventing such extraneous content from being displayed, and then alerting operator personnel and providing specific instructions on subsequent steps to take.

Certain types of attacks, including SQL injections, produce output results that are potentially used or perceived by an attacker to determine the size of the attack surface to initiate and complete attacks. By implementing the concept of non-persistence for selected system components, organizations can provide a known state computing environment for a specific time period that does not give adversaries sufficient time to exploit vulnerabilities in organizational systems and the environments in which those systems operate. Since the APF is a high-end, sophisticated threat regarding capability, intent, and targeting, organizations assume that even an extended period, a percentage of attacks will be successful. Non-persistent system components and services are activated as required using protected information and terminated periodically or at end of sessions. Non-persistence increases the work factor of adversaries in attempting to compromise or breach organizational systems.

Non-persistence can be achieved by refreshing system components by periodically re-imaging components or by using a variety of common virtualization techniques. Non-persistent services can be implemented by using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent). The benefit of periodic refreshes of system components and services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult to determine). The refresh of selected system components and services occurs with sufficient frequency to prevent the spread or impact of attacks, but not with such frequency that it reduces the organization's availability. Refreshes of critical components and services may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

SI-14 (1) 2 System and Information Integrity | Non-persistence / Obtain software and data employed during system component and service refreshes from the following trusted sources: 
   (Assignment: organization-defined trusted sources).

Obtain software and data employed during system component and service refreshes from the following trusted sources:

(a) Obtain software and data from whitelisted, read-only media or from certified software providers.

Tainted sources include software and data from untrusted third parties, untrusted media, or from untrusted sources.

SI-14 (2) 2 System and Information Integrity | Non-persistence / Non-persistent Information

(a) Select: refresh (Assignment: organization-defined information) 
   (Assignment: organization-defined trusted sources) 

Generate (Assignment: organization-defined information or data) and

Obtain information that is no longer needed.

Retaining information longer than is needed makes the information a potential target for adversarial endeavors exercising for high value assets or compromising through unauthorized disclosure, unauthorized modification, or exfiltration. For system-related information, continuous retention provides adversaries advanced warning information that can assist in their reconnaissance and lateral movement through the system.

SI-14 (3) 2 System and Information Integrity | Non-persistence / Non-persistent Correctly

Ensure connection to the system an element and terminate connections after: 
   (Assignment: organization-defined connection at end of use).

Persistent connection to systems can provide advanced adversaries with paths to move internally through systems, and potentially position themselves closer to high value assets. Placing the availability of such connections impedes the adversary's ability to move freely through organizational systems.

SI-15 1 System and Information Integrity | Information Output Filtering

Filter output information from the following software programs and/or applications to ensure that the information is consistent with the expected content: 
   (Assignment: organization-defined software programs and/or applications).

Filtering output information helps reduce the potential for vulnerabilities from system components and services. For example, filtering output information can prevent sensitive information from being displayed, and alerting monitoring tools that anomalous behavior has been discovered.

SI-16 1 System and Information Integrity | Memory Protection

Implement the following controls to protect the system memory from unauthorized code execution: 
   (Assignment: organization-defined controls).

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can be either hardware-enforced or software-enforced with hardware enforcement providing the greatest strength of enforcement.

SI-17 1 System and Information Integrity | Fail-Safe Procedures

Implement the indicated fail-safe procedures when the indicated failures occur: 
   (Assignment: organization-defined list of failure conditions and associated fail-safe procedures).

Fail-safe procedures include loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to take. These steps include doing nothing, reestablishing system settings, shutting down processes, exiting the system, or contacting designated organizational personnel.
SI-18 | System and Information Integrity | Personally Control ID

Correct or delete personally identifiable information that is inaccurate or outdated, as determined by an automated mechanism. The use of automated mechanisms to improve data quality may inadvertently create privacy risks. Automated tools may connect to external or otherwise unrelated systems, and the matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plans. An audit is obtained and used across the information life cycle. It is important to perform the accuracy and relevance of personally identifiable information. Automated mechanisms can augment existing data quality processes and procedures and enable an organization to better identify and manage personally identifiable information in larger-scale systems. For example, automated tools can greatly improve efforts to consistently normalize data or identify enrollees. Automated tools can also be used to improve auditing of data and assist enactors that may inadvertently alter personally identifiable information or incorrectly associate such information with the wrong individual. Automated capabilities boost privacy impact assessment and make determinations at scale and enable more fine-grained detection and correction of data-quality errors.

SI-19 | System and Information Integrity | De-identification | Automation

Display data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems. Data tagging personally identifiable information includes tags noting processing permissions, authority to process, de-identification, impact level, information life cycle stage, and retention or last updated dates. Employing data tags for personally identifiable information can support the use of automated tools to correct or delete relevant personally identifiable information.

SI-19 | System and Information Integrity | De-identification | Data Tags

Collect personally identifiable information directly from the individual. Individuals, or their designated representatives, are the source of correct personally identifiable information about themselves. Organizations consider contextual factors that may incentivize individuals to provide correct data versus providing false data. Additional steps may be necessary to validate collected information based on the nature and context of the personally identifiable information, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of personally identifiable information 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 personally identifiable information.

SI-19 | System and Information Integrity | De-identification | Individual Requests

Correct or delete personally identifiable information upon request by individual or their designated representatives. Persons whose personally identifiable information is maintained by organizations may cause problems for individuals, especially in those business functions where inaccurate information may result in inappropriate decisions or the denial of benefits and services to individuals. Even correct information, in certain circumstances, can cause problems for individuals that outweigh the benefit of an organization maintaining the information. Organizations use discretion in determining personally identifiable information to be corrected or deleted, based on the scope of requests, the changes sought, the impact of the changes, and applicable laws, regulations, and policies. Organizations may consult with the senior agency official for privacy and legal counsel regarding appropriate instances of correction or deletion.

SI-19 | System and Information Integrity | De-identification | Notator of Collection or Deletion

Notify [Assignment: organization-defined recipients of personally identifiable information] and individual that the personally identifiable information has been corrected or deleted. When personally identifiable information is current or deleted, organizations take steps to ensure that all authorized recipients of such information, and the individual with which the information is associated or their designated representative, are informed of the corrected or deleted information.

SI-09 | System and Information Integrity | De-identification

Remove the following elements of personally identifiable information from datasets: [Assignment: organization-defined elements of personally identifiable information]; and b. Evaluate [Assignment: organization-defined frequency] for effectiveness of de-identification. De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. Many datasets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Personally identifiable information is removed from datasets by trained individuals when such information is not or no longer necessary to satisfy the requirements envisioned for the data. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing these statistics are removed. Removing identifiers improves privacy protection, since information that is removed cannot be inadvertently disclosed or improperly used. Organizations may be subject to specific de-identification definitions or methods under applicable laws, regulations, or policies. De-identification is a residual risk with the de-identified data. De-identification efforts can vary including combining new datasets or other improvements in data analytics. Maintaining awareness of potential attacks and evaluating the effectiveness of de-identification over time supports management of this residual risk.

SI-19 | System and Information Integrity | De-identification | Collection

De-identify the dataset upon collection by not collecting personally identifiable information. If a data source contains personally identifiable information but the information will not be used, the dataset can be de-identified upon creation by not collecting the data elements containing the personally identifiable information. For example, if an organization does not intend to use the social security number of an applicant, then application forms do not ask for a social security number.
A motivated intruder test is a test in which a person or group takes a data release and speculates on re-identification by using non-deterministic noise to the results of mathematical operations before the results are reported. The mathematical definition for differential privacy holds that the result of a dataset analysis should be approximately the same before and after the addition or removal of a single data record (which is assumed to be the data from a single individual). In its most basic form, differential privacy applies only to online query systems. However, it can also be used to produce machine learning statistical classifiers and synthetic data. Differential privacy comes at the cost of decreased accuracy of results, forcing organizations to quantify the trade-off between privacy protection and the overall accuracy, usefulness, and utility of the de-identified dataset. Non-deterministic noise can include adding small random values to the results of mathematical operations in dataset analysis.

Software that is claimed to implement a validated algorithm may contain bugs or may implement a different algorithm. Software may de-identify one type of data, for example, integers, but not another type of data, for example, floating point numbers. For these reasons, de-identification is performed using algorithms and software that are validated.

A motivated intruder test can determine if de-identification is insufficient. It can also be a useful diagnostic tool to assess if de-identification is likely to be sufficient. However, the test alone cannot prove that de-identification is sufficient.
SR-1 1 Supply Chain Risk Management | Policy and Procedures

1. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   a. A plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];
   b. Supply chain risk management plans for the following systems, system components, or system services: [Assignment: organization-defined supply chain risk management plan(s)];
   c. Supply chain risk management plans consistently across the organization; and
   d. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threats, organizational or environmental changes.

2. Procedures to facilitate the implementation of the supply chain risk management policy and associated supply chain risk management controls:
   a. Designate or [Assignment: organization-defined effort] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
   b. Revisit and approve the current supply chain risk management plan [Assignment: organization-defined frequency].

SR-2 1 Supply Chain Risk Management | Supply Chain Risk Management Plan

1. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of the following systems, system components, and system services: [Assignment: organization-defined systems, system components, or system services];

2. Procedures [Assignment: organization-defined frequency].

SR-3 1 Supply Chain Risk Management | Supply Chain Controls and Processes

1. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain partner(s)];

2. Document the selected and implemented supply chain processes and controls in [Assignment: organization-defined supply chain risk management plan].

3. Supply chain elements include organizations, entities, or tools employed for the development, acquisition, delivery, maintenance, sustainment, or disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools and techniques; and measures to maintain assurance or other processes, programs, or procedures associated with the development, acquisition, maintenance, and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Document</th>
<th>Related Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR-4 (2)</td>
<td>2</td>
<td>Supply Chain Risk Management</td>
<td></td>
<td>Implement the following supply chain controls to reduce harm from potential adversaries identifying and targeting the organization's supply chain: (Assignment: organization-defined controls).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of system or non-standardized configurations; employing approved vendor lists with standing relationships in place; following pre-agreed maintenance schedules and updates and patch delivery mechanisms; maintaining a contingency plan in case of a supply chain event; and using procurement cover costs that provide exclusive to commitments or obligations, using diverse delivery routes; and retaining the time between purchase decisions and delivery.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR-4 (1)</td>
<td>2</td>
<td>Supply Chain Risk Management</td>
<td></td>
<td>Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: (Assignment: organization-defined systems, system components, and associated data). Every system and system component has a point of origin and may be changed throughout its existence. Provenance is the chronology of the origin, development, ownership, location, location, and changes to a system or system component and associated data. It may also include personnel and procedures used to interact with or use modifications to the systems, components, or associated data. Organizations consider developing processes (see SR-4) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preparing and monitoring for automatic changes to the provenance records. Organizations consider developing methods to document, maintain, and maintain valid provenance baselines for systems, system components, and related data. Such actions help track, assess, and document changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR-4 (2)</td>
<td>2</td>
<td>Supply Chain Risk Management</td>
<td></td>
<td>Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: (Assignment: organization-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components). Knowing who and what is in the supply chain of an organization is critical to gains visibility into supply chain activities. Visibility into supply chain activities is also important for monitoring and identifying high-risk procurement activities. Without reasonable visibility into supply chain elements, processes, and personnel, it is very difficult for organizations to understand and manage risk, and ultimately reduce the susceptibility to adverse events. Supply chain elements include organizations, entities, or tools used for the development, acquisition, delivery, maintenance, and disposal of systems and system components. Supply chain processes include development processes for hardware, software, and firmware; shipping and handling procedures; configuration management tools, techniques, and measures to maintain provenance; personnel and physical security programs; or other programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain personnel are individuals with specific roles and responsibilities related to the secure development, delivery, maintenance, and disposal of a system or system component. Identification methods are sufficient to support an investigation in case of a supply chain change (e.g., if a supply company is purchased, components, or event).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR-4 (1)</td>
<td>2</td>
<td>Supply Chain Risk Management</td>
<td></td>
<td>Validate as Genuine and Not Altered</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or component; using blurred or filtered buys; requiring tamper-evident packaging or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or hardware, and your development practices throughout the system development life cycle. Organizations also consider providing incentives for suppliers who implement controls; promote transparency into their processes and security and privacy practices; provide contract language that addresses the prohibition of tainted or counterfeit components; and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and promoting development plans, documentation, and evidence communications are the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR-5 (1)</td>
<td>2</td>
<td>Supply Chain Risk Management</td>
<td></td>
<td>Display the following controls to ensure adequate supply of [Assignment: organization-defined critical system components]: (Assignment: organization-defined controls).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Organizations can attempt to impede operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component risks how to mitigate the loss of temporary or permanent systems. Controls to ensure that adequate supplies of critical system components include the use of multiple suppliers throughout the supply chain for the identified critical component; stockpiling spare components to ensure operation during mission-critical times; and the identification of functionally-identical or similar components that may be used, if necessary.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**

- IA-2, IA-8, PE-16
- SA-4, SA-10, SA-11
- SR-6, MA-2, MA-4, MA-19
SR-4 (1) 2 Supply Chain Risk Management | Acquisition Strategy, Tools, and Methods (Assessments Prior to Selection, Acceptance, Modification, or Update) Avoids the system, component, or system service prior to selection, acceptance, modification, or update.

Organizations personnel or independent, external entities conduct assessments of systems, components, products, tools, and services to uncover evidence of tampering, unintentional and intentional vulnerabilities, or evidence of non-compliance with supply chain controls. These include malicious code, malicious processes, defective software, backups, and counterfeit. Assessments can include evaluations; design proposal reviews; visual or physical inspections; static and dynamic analyses; visual, x-ray or magnetic particle inspection; simulations; white, gray, or black box testing; test testing; stress testing; and penetration testing (see SR-6(1)). Evidence generated during assessments is documented for follow-on actions by organizations. The evidence generated during the organizational or independent assessments of supply chain elements may be used to improve supply chain processes and to inform the supply chain risk management process. The evidence can be reviewed in follow-on assessments. Evidence and other documentation may be shared in accordance with organizational agreements.

SR-6 1 Supply Chain Risk Management | Supplier Reviews Review the supply chain related risks associated with suppliers or contractors and the system, system component, or system service they provide (Assessment: organization-defined frequency).

A review of supplier risk includes security processes, foreign ownership, control influence (FOCI), and the ability of the supplier to effectively assess any subordinate second-tier and third-tier suppliers and contractors. The review may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor. Organizations use any open-source information to monitor for indications of theft information, foreign development and quality control practices, information theft, or counterfeits. In some cases, it may be appropriate to share review results with other organizations in accordance with any applicable inter-organizational agreements or contracts.

SR-8 1 Supply Chain Risk Management | Communication Operations Security (OPSEC) controls

Implement the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service (Assessment: organization-defined Operations Security (OPSEC) controls).

Supply chain OPSEC expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process that includes identifying critical information; analyzing friendly actions related to operations and other activities to identify those actions that can be observed by potential adversaries; determining indicators that potential adversaries might obtain that could be interpreted or pieced together to derive information in sufficient time to cause harm to an organization; implementing safeguards or countermeasures to eliminate or reduce exploitable vulnerabilities and thus risk to an acceptable level; and, finally, considering how aggregated information may expose any specific use of the supply chain. Supply chain information includes user identities; user for systems, system components, and system services; supplier identities; security and privacy requirements; system and component configurations; supplier processes, design specifications, and testing and evaluation results. Supply chain OPSEC may require organizations to withdraw mission or business information from suppliers and may include the use of intermediaries to hide the end use, or use of systems, system components, or system services.

SR-8 1 Supply Chain Risk Management | Notification Agreements Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the Selection (one or many) notification of supply chain compromises; results of assessments or audits (Assessment: organization-defined information).

The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components, is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result or could be used to help the supply chain entity resolve a concern or improve its processes.

SR-9 1 Supply Chain Risk Management | Tamper Resistance and Detection Implement a tamper protection program for the system, system component, or system service.

Anti-tamper technologies, tools, and techniques provide a level of protection for systems, components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.

SR-9 (5) 2 Supply Chain Risk Management | Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle Apply anti-tamper technologies, tools, and techniques during multiple stages in the system development life cycle, including design, development, integration, operations, and maintenance.

Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitution easier to detect and therefore less dangerous.

SR-10 1 Supply Chain Risk Management | Inspection of Systems or Components Inspect the following systems or system components: Selection (one or more) at random; or (Assessment: organization-defined frequency), upon (Assessment: organization-defined indicators of need for inspection) to detect tampering (Assessment: organization-defined systems or system components).

Inspection of systems or system components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components that are out of organizational control areas. Indications of a need for inspection include when individuals return from travel to high-risk locations.

SR-11 1 Supply Chain Risk Management | Component Authenticity Source (Calculation: organization-defined techniques and methods), deploy (Calculation: organization-defined techniques and methods).

Proper disposal of system components helps to prevent such components from entering the supply chain.
<table>
<thead>
<tr>
<th>Control ID</th>
<th>Level</th>
<th>Control Name</th>
<th>Withdrawn</th>
<th>Control Text</th>
<th>Discussion</th>
<th>Related Controls</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR-11 (4)</td>
<td>2</td>
<td>Supply Chain Risk Management</td>
<td>Component Authenticity / Anti-counterfeit Scanning</td>
<td>Scan for counterfeit system components [Assignment: organization-defined frequency].</td>
<td>The type of component determines the type of scanning to be conducted (e.g., web application scanning if the component is a web application).</td>
<td>RA-5</td>
<td></td>
</tr>
</tbody>
</table>